Journal of Education for Pure Science- University of Thi-Qar
Vol.13, No.3 (Sept.2023)
Website: jceps.utq.edu.iq Email jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.10.01.01

Securing Transactions Using Hybrid Cryptography in E-commerce Apps

Ghanima Sabr Shyaa1 **Mishall Al-Zubaidie*1**

[1, 2, 3] Department of Computer Science, College of Computer Science and Mathematics, University of Thi-Qar, Iraq

Received 17/7/2023, Accepted 6/8/2023, Published 21/9/202

Abstract:

The development of technology at the present time leads to an increase in the use of electronic commerce due to the increase in demand processes, whether selling or buying goods, products, services, or payment requests, and that the transfer of information the merchants is sensitive and important information, and this information or operations may be subject to penetration or attacks. In this research, we designed a protocol that integrates the Fernet algorithm and the ElGamal algorithm, and we use the Data Leakage Detection Technology (DLD) to safeguard e-commerce transaction data. This protocol provid high security for information, and the integration of algorithms provides high security and strong performance for information transactions that are difficult to hack. We incorporate encryption algorithms to achieve a high level of security and performance. The proposed protocol is higher in security and performance than the algorithms of previous studies.

Keywords: ElGamal; E-commerce apps; Fernet; Hybrid Encryption; Information Protection; Lightweight Process; Symmet Encryption

Introduction:

Electronic commerce (often referred to as "E-Commerce") is the act of acquiring, supplying for sale, or trading goods, services, and information over a computer network. E-commerce is a part of e-business, which is defined more broadly and includes extends beyond merely commerce to include things like customer service, business partnerships, job openings, etc. Database or database technology is needed for e-commerce in addition to web network technology, email, and other non-computer technologies, like systems for transporting goods and payment options for online shopping. Buying and selling activities are collectively referred to as "e-commerce" sometimes known as electronic commerce, as well as the electronic marketing of services, goods, and information.

Utilizing an electronic system, such as a computer network, television, radio, or the internet, to purchase, sell, and market goods and services [1]

Electronic commerce is becoming more popular around the world as an essential and inevitable practice result of the most recent innovations in the information and communication technology area. One of the most significant ICT (information and communication technology) applications, e-commerce is a component of the knowledge economy, which nations need to be aware of in order to stay up with the current environment and advancements enforced by its representatives. In the expanding popularity of e-commerce. The idea of the "e-merchant" who primarily uses e-commerce applications to meet his needs and wishes, has been linked to e-commerce. Retaining customer and merchant information is very important in e-commerce and online transactions, which is sensitive and important for the personal information of the merchants [2].

The security aspect of e-commerce is an important factor, to prevent unwanted things such as data leakage and financial losses. Protecting merchant information and protecting transactions in e-commerce is of the utmost importance. The increasing use of e-commerce. This means that more people have entered their personal information into applications, one method of protecting private data during e-commerce transactions data security merchant works to protect personal transaction information from hackers a common security requirement authentication, merchant information, data confidentiality, data integrity and non-repudiation. The protection of information is the main objective of these security measures [3].

Since security attacks are linked to online shopping, encryption is used there, for e-commerce transactions, using encryption offers a framework that is both extremely safe and productive from public and private encryption technologies such as DES, RSA, TWOFISH, there are weaknesses in these algorithms are the RSA algorithm is slow and the mathematical operations are large, TWOFISH algorithm is more complex compared to other old standards such as DES, this affects security transactions [4].

Personal information must be kept secure to minimize risks. Among the most important risks or attacks to which information is exposed are: Snooping, pharming, dictionary attacks, and impersonalization, these attacks attempt to penetrate transaction information or penetrate personal information by vishing and stealing customers' personal information in e-commerce transaction applications [5]. Transactional information is exposed to types of penetrations or attacks in electronic commerce applications. Were through mobile phones or through websites through the internet, it becomes a security issue a basic task. In this research, we proposed encryption algorithms, ElGamal algorithm and Fernet algorithm.

Our main “contribution to this research”:

• We design a robust protocol that achieves lightweight, high-performance encryption operations through ElGamal algorithm for key generation and fernet algorithm for information encryption and decryption operations.

• We design a robust protocol that achieves a balance between performance and security in e-commerce applications.

• Testing performance of the proposed protocol and the e-commerce application transaction protocol in the SCYTHER tool that proof, the proposed protocol provid more than the previously protocols.

1. Related Works

Existing research addressed issues of using symmetric and asymmetric encryption algorithms in e-commerce applications, but the existing schemes still contain many security and performance flaws. This section will review the recent research related to the topic of our research in an extensive manner.

Sidik et al. [6] suggested a technique the one-time pad algorithm's flaw can be concealed by altering each cipher text the three pathways used in the three passes protocol method. In order to modify cipher text, the cipher-text is first encrypted combining the RSA and ElGamal algorithms to produce super cipher text. The RSA algorithm is used to encrypt the first and third lines, and encryption is done with the ElGamal algorithm the second line. There are several problems, including that the proposed algorithm uses large initial numbers and makes complex operations and the use of more than one key and different lengths, the one-time pad algorithm is breakable due to utilizing a single key for a single operation, and the key is easy to crack.

Ali et al. [7] submitted a proposal for development a trustworthy algorithm for multi-factor authentication for mobile payment systems. To increase security when authenticating mobile money, they used a cutting-edge strategy that combined PIN, an OTP, and a biometric fingerprint. Additionally, to validate a mobile money withdrawal, they used a quick response (QR) code and biometric fingerprint. The security of the PIN and OTP is enforced by Fast Identity Online (FIDO), which employs a biometric fingerprint and RSA standard public key cryptography in addition to Fernet encryption to secure a QR code and the data in the databases, there are a proposal Weaknesses, including that the RAS algorithm is complex and large mathematical operations. This leads to system slowdowns. Also, the fingerprint may change due to external conditions such as exposure to burns and diseases. This affects the proposed system.

Tyagi [8] submitted a proposal protection data in cloud computing, especially images Double-level encryption using CNN Auto-Encoders was achieved by combining "AES" and "Fernet", bitmap images are produced as outputs once the source images have been processed, encrypted, and decrypted, which users can then decrypt using a "key" as necessary. There are several problems, including this double encryption level that affects performance, data and information are exposed to theft and damage when stored in cloud computing.

Dong [9] proposed using sensor technology smart platform e-commerce data will be mined and analyzed, after which a new mobile e-commerce platform will be designed and built, using Jingdong and Taobao, two of the biggest e-commerce sites, as examples Through online evaluation surveys and research, it was determined the importance of elements affecting the caliber of logistics services and customer satisfaction under various logistics distribution models. However, there are several weaknesses. Customer satisfaction depends on the quality of goods service, its quality, delivery time, speed of delivery, and the delivery staff's attitude. There is a difference in delivery and delivery time, this affects the e-commerce platforms. The three-level system construction model increases the interaction between the user and the server, except the dynamic page simultaneously contains both the performance and the generated data, it results in a very huge dynamic page and makes it simple

for logical processing to become confused, not only does it pose security risks to the system, but it also makes system development and maintenance difficult.

Abdul Hussien et al. [10] suggested an agent program can be installed on each customer device to manage the purchase and security process without the need for customer involvement. This environment uses an encryption algorithm to produce an encryption algorithm that strikes a balance between time and complexity. Numerous improvements are made to the AES encryption algorithm. Preprocessing steps (zigzag and padding) have been added, the sub byte step has been eliminated, and the number of rounds has been decreased. The performance (security and speed) of the AES was chosen because it is suited for encrypting transferred data over the internet. The proposed system suffers from huge arithmetic operations. This leads to a decrease in algorithm speed and is costly and a difference in increasing the size of the file memory.

Kota [11] proposed hybrid encryption to store data and cloud computing, the AES-GCM, Fernet, AES-CCM, and CHACHA20 POLY1305 algorithms are used to secure data block by block. The technique is generally used for key information security, and the algorithm key size is 128 bits. There are N parts to one file. Each and every part of the file is encrypted with a special algorithm. All files are encrypted concurrently using two distinct techniques. For the purpose of file decryption, the encryption process is reversed. This proposal has some problems, including that GCM-AES used to encrypt file segments takes minimal time and compared to other similar algorithms, has the highest throughput for encryption and decryption, and that the process of dividing files into parts and each part performs a different algorithm makes large and complex calculations.

Koppaka and Lakshmi [12] presented a proposal using encryption algorithms is hyperchaotic sequence and the ElGamal algorithm were integrated, effectively encrypting the data that was outsourced and reducing the system's computing complexity, using IEC algorithm. The classic ElGamal algorithm is combined with pseudorandom sequences for a pseudorandom key generation, and the IEC technique significantly increases the data security in cloud situations by enhancing the strength of key pairs. There are several weaknesses, including that the IEC algorithm contains different lengths of keys. This makes operations complex. The performance of the algorithm depends on execution time, encryption and decryption times, as well as the time required for key generation. This affects system performance and the system computational complexity.

Charles et al. [13] suggested proposed using a newly generated private key and a public key for decryption, the ElGamal encryption decryption method has been upgraded to better protect the data. The encrypted data is then decrypted in response to a user's request for it, with ResNet-50's nearly 50-layer convolutional neural network classifier. The categorization or refinement process is carried out. The UCI heart disease repository's dataset on cardiovascular disease. However, user data may be exposed to types of attacks that are sensitive and personal information. Res Net is costly when examining a lot of parameters.

Ahmed [14] presented a proposal to use encryption algorithms to protect networks and devices connected to each other. Quick and trustworthy communication without interruption of continuance between lot devices is a great challenge, by comparing algorithms in terms of key size, message size and execution time. There are some vulnerabilities in the long key RAS algorithm. This causes delays in encryption and complex operations. ECC is slow in public key operations. The algorithms may be subjected to attacks that affect its performance.

Parvathi et al. [15] presented a suggestion using Fernet (AES encryption algorithm) with blockchain technology in the food supply chain, this makes transactions safe between farmers as well as consumers/buyers. However, this technology suffers because it takes time to process data for each purchase and sale order process, and this affects system performance, as there will be delays in orders and damage to goods.

2. The importance of the Merchant in Electronic Commerce Transactions.

E-commerce is known as commercial transaction, conducted electronically in facilitating both marketing and stalking operations anywhere, anytime and with whoever participates in the transaction. Transactions over the internet. This adaptability is what attracts customers and merchants can expand sales of their products by partnering with multiple websites. Customers can buy goods and/or services directly from online retailers. Merchants deal on a day-to-day basis on the merchant's website. Daily deals they sell goods and services to customers for a fee, coupons on the site. Online market merchant offers to sell goods or services by uploading data or information that will be sold in online stores via online shopping malls [16]. E-commerce provides a number of merchants and platforms via the internet, and the merchant is responsible for the quality of the product, the quality of sales, and its price. Internet platforms have a direct impact on the financial gains of platform merchants, whereby screening, curating, and managing user interactions have transparent, flexible management limits on platform merchants. For instance, online marketplaces like Amazon, Alibaba, and eBay bring together a large number of users and vendors and have a huge impact on the content selection, categorization, and display. The caliber of the goods that the merchants sell. It corresponds to advertising, whereas the violation procedure results in the sellers' daily sales process displaying deceptive advertising and subpar goods of promoting goods and commodities in e-commerce transactions [17]. Pricing affects sales volume and is determined by the merchant. Consumers delegate with merchants about product prices. Social media advertising, consumer engagement for products in social media, increase merchant sales while earning commission and the merchant spends money on search engine marketing to promote suggested products before consumers [18].

There have been a lot more deals, and there are opportunities to make purchases through internet sales.

1. Consumers and e-merchants interact online via a server that the e-merchant has rented from an Internet service provider (ISP).
2. Terms of use and terms of sale, or terms standard, are included with all online transactions. E-merchants typically post these terms on their websites, and interested e-customers must simply click the accept button.
3. Accepting electronic clients via the mechanism for clicking the physical representation of a contract that, of course, binds the electronic merchant.
4. Following the completion of the contract by the two parties, the payment procedure, which involves two intermediary banks from the commercial bank that is acquiring the party and the bank's issuing bank, respectively. The client mechanism authorizes the e-issuing customer's bank to make several payments to the informed the purchasing merchant's bank to the e-commerce site on behalf of the customers for the cost of the items.
5. After the payment procedure is complete, the e-merchant can proceed with fulfilling its obligations in the form of delivering the items in line with the timing and product specifications that

were agreed upon [19].

The importance of the merchant in electronic commerce is to protect the security of information, customer data, product data, and protection from theft, and this is done through the use of built-in encryption techniques that provide high data security and promotion of products in the best ways and quality of goods.

3. Basic Concepts About Applied Cryptography Mechanisms

In this section, we will provide the basic details of the algorithms adopted in this research.

3.1 ElGamal algorithm

One of the first and most well-known public key encryption systems is the ElGamal cryptosystem. It gained widespread popularity in the 1980s and 1990s because it was both effective and patent-free [20]. ElGamal is a well-known encryption algorithm. Messages are often encrypted using the ElGamal method. Using random integers to compute key creation is a relatively secure method because the ElGamal algorithm comprises a straightforward and effective cryptographic procedure that can do several factoring operations. As a result, ElGamal can shield messages from threats to computer networks like websites and online sites as well as cryptanalyst assaults that try to damage computer systems and computer networks as a whole [21]. Public and private keys are used in the encryption and decryption procedures of the ElGamal algorithm, a type of asymmetric cryptography. The only device that will store information about both buttons is internal. The security of the ElGamal algorithm depends on the computational complexity of discrete logarithms. The key ElGamal algorithm is created using the following steps:

p = primes and $y = g\ x\ mod\ p$ stands for random numbers, where $g < p$. Conditions: x = random numbers, $g, x < p$ The following is how text is encrypted: $a = g\ k\ mod\ p$, where k is a random number decrypting text involves the following steps.: $m = b * a\ (p - 1 - x)$ mod p [22]. The ElGamal cryptosystem is a very effective application of Diffie-Hellman algorithm, the cipher text for a particular message m is not repeated due to randomness in the enciphering process. The utilization of the residual when a very large number is split by a prime number is the distinctive feature of the ElGamal algorithm's encryption and decryption. There are an unlimited of ways to divide the number, therefore it would be exceedingly difficult to identify the original, special combination of these two factors that produced that residual [23]. The key size utilized by ElGamal's approach will eventually be used to determine the positive prime number p and the integer q, which is p primitive root. For example, a low parameter will be used to increase accuracy and make calculations simpler. A key length of 1024 bits has been chosen as the parameter [24].

3.2 Fernet algorithm

Fernet is a cryptography technique that offers a straightforward mechanism for authenticating and encrypting data employing symmetric AES-128 in CBC (Cipher Block Chaining) mode with PKCS7 padding to allow various lengths of 128 bits (16 bytes) and using HMAC and SHA256 for authorization [25]. The Fernet algorithm making sure that the data is encrypted makes it impossible for it to be modified or decoded without the key. utilizing the most recent standards. A symmetric encryption and decryption system called Fernet authenticates messages so that the recipient can tell

whether or not they have changed from the version that was originally transmitted. A rookie developer may make several blatant mistakes when building such a system. By providing a secure technique for creating keys (which is equivalent to a password), Fernet avoids these selecting the efficient encryption technique AES and strengthening the encryption by providing a secure "salt" value at random using CBS mode and PKCS7 padding. To avoid tampering, the communication is signed (using HMAC and SHA256). Fernet offers either symmetrical or private keys are a type of cryptography that calls for the safekeeping of a single key that is used for both encryption and decryption. Furthermore, due to its limitations with regard to huge files, executes a single memory load of the entire buffer [26]. The Fernet keys made sure that an encrypted template file could not be revealed or read without the secret key, making it challenging for an attacker to get around or access the database server [27]. A symmetric key approach is used to ensure that without the password key, the encrypted transmission cannot be changed, brute-forced, or decoded. every single reserved, illegible, or non-ASCII character are substituted in this key due to its base64 URL-safe encoding. It makes sure that the keys are handled correctly and that no mistakes happen that an attacker would try to take advantage of. The public-key cryptography standard number 7 (PKCS7) padding and Fernet additionally employs the 128-bit cipher block chaining (CBC) mode of the advanced encryption standard (AES). In order to fill in the vacant bits, PKCS7 padding is employed, and the cipher is therefore in multiples of 128 bits. HMAC, short for hash-based message authentication code, which is used by the password key, is used. The HMAC performs two tasks at once, confirming a message's authenticity and integrity. HMAC was combined with a straightforward 256-bit hashing algorithm (SHA256) in order to increase security [28].

3.3 Data leakage detection technique

Data Leakage Detection (DLD) commonly described as any method or procedure that detects the illegal leakage of sensitive information. Data leakage detection systems (DLDSs) are specialized tools that can track and safeguard personal information, spot instances of data misuse, and locate the nefarious party behind the leak, data leakage can occur intentionally or accidentally dissemination of private or confidential information or data to a harmful, uninvited party. An entity's sensitive data must be distributed to multiple stakeholders by a data distributor, including clients, employees, and business partners inside or outside the location of the organization, for the purpose of conducting business. However, the recipient may abuse this information and leak it, either intentionally or unintentionally, to a few uninvited third parties [29]. Since data must be safeguarded from unauthorized access, data leaking is a significant problem in today's business environment. This uncontrolled data leak exposes businesses to risk. Once this data leaves the domain, the company is in serious danger. Today, a single attack on one company can have an impact on tens of thousands, numerous thousands or even millions of distinct customers, along with even more distinct data [30]. Data leaking has grown to be a big problem for organizations nowadays that goes unnoticed. Data leaking occurs from a variety of sources, which most individuals are unable to identify [5]. Commercial enterprise was resulting in exposure of this unmanageable information leak. If this information disappears, the company faces serious risks. These days, the business is not confined to a small location but is expanding globally. You can electronically transfer this sensitive information using USB keys, spreadsheets, web pages, and other technological devices. Therefore, it becomes

increasingly important to address data security if one client delivers information from a nation to another client through some agents. The corporation might lose a lot of money if the data is released.

Process for Detecting Data Leaks:

1. The distributor enters their login information.

2. The distributor enters the data (for instance, text files) into the database.

3. After logging into the system, the agent requests a specific file, or the distributor uploads all files for the agents appropriately, along with the private key.

4. The distributor delivers the desired file to the requested agents, who then add some fictitious objects.

5. According to his demands (explicit requests or sample requests), agents will download the files.

6. The distributor will search for the leaked data and locate the file if any agents (Fake Agents) release the information to a third party [31].

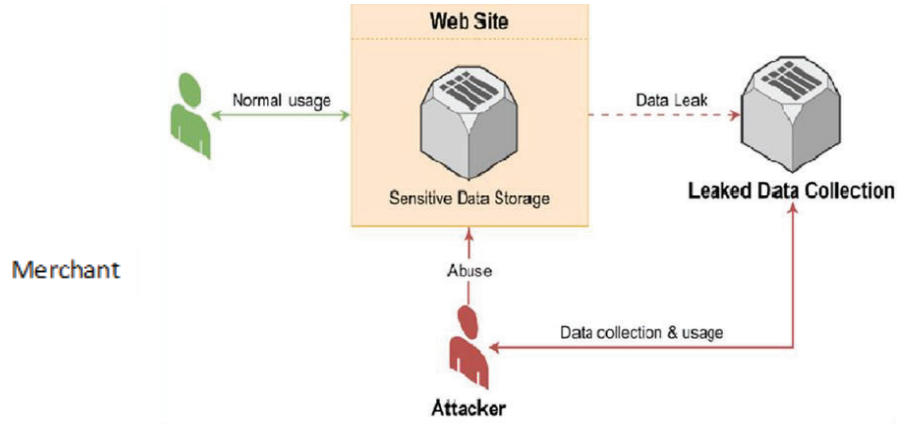

Figure 1: Data leakage detection technique [31].

4. Proposed Protocol to Secure E-commerce Transactions

The spread of wireless communication networks, the use of credit cards and smartphones, the expansion of online shopping, and the continued expansion of the e-commerce market are all driving increased product sales and delivery. Both suppliers and products are part of an e-commerce system. Domains of the Internet, online shopping malls (websites), servers, payment methods, product delivery, and customers. Transactional information may be exposed to breaches or threats on the other hand. Protecting information is important to maintain the security of electronic commerce transactions. We use a high-performance and security protocol to protect information. The general model of the proposed system includes a group of customers providing merchants, payment gateway operations, payment gateway methods, banking services and online sales operations. Figure (2) shows the proposed system. In this proposal, we focus on the order processes between the merchant

and his organization, and how to protect the merchant's information by using symmetric and asymmetric encryption algorithms and data leakage detection (DLD) technology to find out the data leakage in the e-commerce order through the procedure of key generation, decryption and encryption, where this diagram (1) shows the methodology of the system

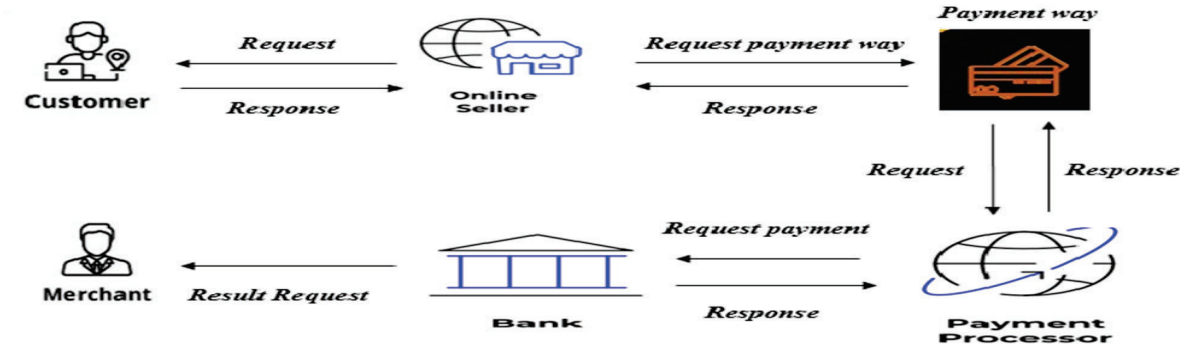

Figure 2: shows a proposed system

5. Implicated symmetric and asymmetric cryptography

In this section we explain the techniques that we use in our proposed system protocol ElGamal, Fernet and DLD:

5.1 ElGamal algorithm

In our protocol, we use an asymmetric algorithm consisting of two keys, public and private, to generate large random keys to increase the security of electronic commerce transactions. We use the ElGamal algorithm because of its high efficiency in generating random keys of different lengths and sizes.

In the proposed protocol, we use the key size is 1024, we divide the pudlic key using the XOR process, we get a secret key size of 256, and we use it for encryption and decryption operations with the Fernet algorithm. We use ElGamal to generate public and private keys.

The following steps provide a description of the key generation process:

• Select a large prime number at random q.

• Select a random number g, which referred random multiplicative to as a generator component

• Select a third number at random x from $\{1 \ldots q-1\}$ as the private key.

• Calculate y by using the formula: $y = g^x \bmod q$ as the public key.

• x should be kept secret as a private key, q, g and y are published as public keys.

The public key is (K_u) and the private key is (K_r).

We use data leakage detection technology during the process of creating the keys, we divide the public key into four parts, and with the addition of the merchant ID number for each key and the XOR operation for each key, we get the public key encryption and decryption using Fernet algorithm.

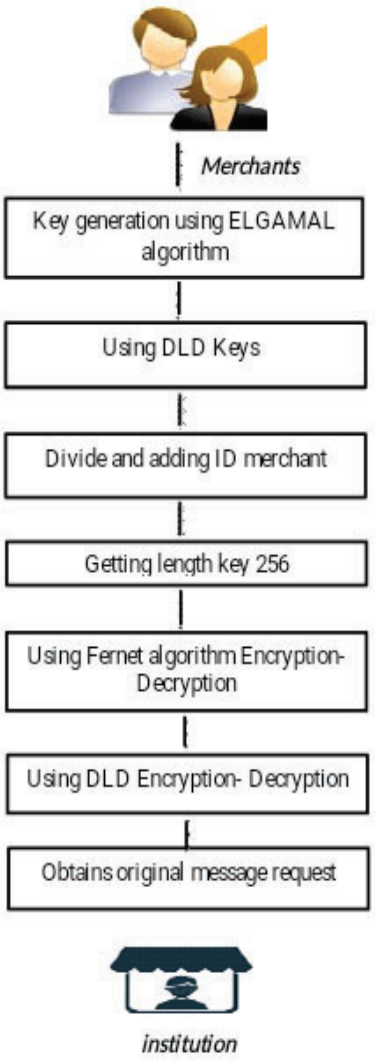

Diagram (1) shows the methodology of the system.

5.2 Fernet algorithm

The Fernet algorithm encrypts and decrypts product sales, delivery orders, and payment gateway paths between merchant (*M*) and trust server (*TS*) with a key length of 256 and salt values to increase randomness and provide more security. Our protocol achieves lightweight and high security operations by using the Fernet algorithm which provides high security for merchant information and protection of information from hacking and e-commerce transactions. The following Figure shows the general Fernet architecture

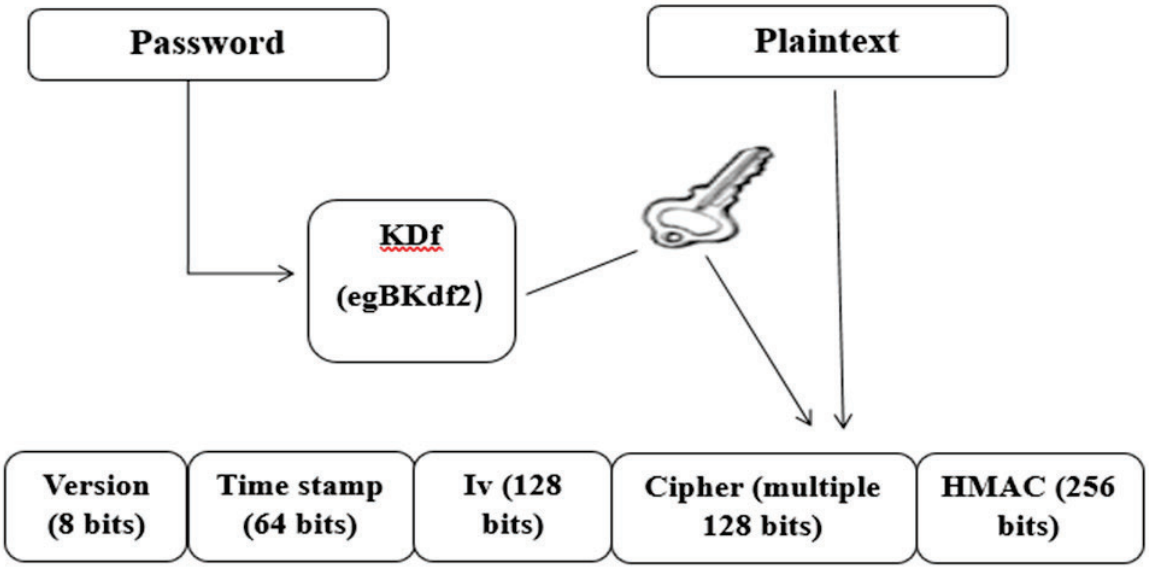

Figure 3: the general Fernet architecture.

5.3 Data leakage detection

Data may expose clients such as merchants to hacking by an unauthorized person or vulnerable to attacks, and information is sensitive when the transmission of this information leads to data leakage. To protect this data, when a merchant sends a request to a company's website to search for a product, the merchant's information must be protected. Sensitive and important information may lead to data leakage from a third party, such as agents responsible for data transmission merchants, or if any error occurs in the order data, we use this technology in our protocol to detect data leakage in the process of creating keys and the encryption and decryption process. By adding dummy objects that are not real, but real agents to the distributed data, it helps to find out who is responsible for the leak and may be a guilty agent. Let's U represents the group of merchants and C the group data group within the company in case the agent is at fault. G_a represents the sum of the agents guilty and a represents the agent, and we must ascertain the probability that the agent is guilty. Leakage data represent L represents a probability by $P_b = G_a \mid L$. We suppose that $\forall Si \in L$, where S represents sensitive data from the dataset $I= \{\upsilon_1, \upsilon_2..., \upsilon_n\}$, can only be accomplished in one of two ways. The first is that any agent from the set of $Si = \{a \mid Si \in X j\}$, where Si is the set of agents possessing Si in their allocated dataset $X j \ \forall j= \{1, 2..., m\}$, has leaked Si to target t or the target t has independently retrieved without the aid of any agent a, the data Si by guess or by any other technique. A measure of how likely it is that any data object Si will escape the leak dataset L. In other words, if it is leaked by any

agent, P_b "leak *Si* to *L*" equals $a \in Si$, but P_b "leak *Si* to *L*" equals if it is obtained by the target *t*. We think that *a* decision to reveal any information *Si* is independent of the decision to leak any additional information *Si*. The agent *a* probability of guilt ($P_b\ G_a \mid L$) is calculated as shown below:

$$P_b\{G_a|L\} = 1 - \prod_{si \in L \cap Xj} 1 - \frac{(1-a)}{csi} \text{----------(1)}$$

5.4 Purchase and Payment Request

perform cryptographic operations based on the Fernet algorithm for a set of cryptographic orders, and there are order forms that include purchase and payment orders. Figure (4) shows the types of requests. Order request information, whether it is a purchase order or a payment order, has been encrypted depending on the type of order. The order forms used in this research are real forms of e-commerce order forms such as purchase orders and payment requests, which are taken from free databases on the Internet [32], and do not contain information of a specific party such as a company, institution or personal information. In order to perform the process of encrypting and decrypting purchase and payment orders, we have added some personal information and non-real order data of users. We encrypt an order received from a merchant based on the Fernet method and then send it to a server and the personal information of each of the merchants is protected.

BUSINESS RECEIPT

Company Name: _____
Street Address: _____
City, State, Zip: _____
Phone: _____
Fax: _____
Email: _____

Date: _____ Receipt #: _____

QTY	Description	Unit Price	Total

Subtotal: _____
Tax Rate: _____
Tax: _____
Total Amount Due: _____
Amount Paid: _____

Customer/Client Information

Name: _____
Street Address: _____
City, State, Zip: _____
Phone: _____
Email: _____

Payment Method:
☐ Credit Card (No. _____)
☐ Cash
☐ Check (No. _____)
☐ Other: _____

Authorized Signature _____

Title: _____

YOUR LOGO

PURCHASE ORDER

Company Name
123 Main Street
Hamilton, OH 44416
(321) 456-7890
Email Address
Point of Contact

DATE 01/18/2022
PURCHASE ORDER NO. A246
CUSTOMER NO. 114H

BILL TO
ATTN: Name / Dept
Company Name
123 Main Street
Hamilton, OH 44416
(321) 456-7890
Email Address

SHIP TO
ATTN: Name / Dept
Company Name
123 Main Street
Hamilton, OH 44416
(321) 456-7890

SHIPPING METHOD	SHIPPING TERMS	SHIP VIA	PAYMENT	DELIVERY DATE

ITEM NO.	DESCRIPTION	QTY	UNIT PRICE	TOTAL
A111	Women's Tall - M	10	$10.00	$100.00
B222	Men's Tall - M	5	$20.00	$100.00
C333	Children's - S	10	$5.00	$50.00
D444	Men's - XL	5	$10.00	$50.00
				$0.00
				$0.00
				$0.00
				$0.00
				$0.00
				$0.00
				$0.00

Remarks / Instructions:

SUBTOTAL 300.00
enter total amount DISCOUNT 50.00
SUBTOTAL LESS DISCOUNT 250.00
enter percentage TAX RATE 7.214%
TOTAL TAX 18.04
SHIPPING/HANDLING 50.00
OTHER 50.00
TOTAL $ 368.04

Please make check payable to Your Company Name.

THANK YOU

AUTHORIZED SIGNATURE DATE

Figure (4): Purchase and payment Request.

5.5 Proposed protocol procedures

In designing the protocol, we rely on the method of encrypting and decrypting request transactions. This is done using symmetric and asymmetric encryption algorithms. We use the Fernet algorithm to encrypt the text and request information. We following the next steps:

1. We generate random keys that are the private and public keys by default using an ElGamal asymmetric encryption algorithm. Then we divide the random key whose size is 1024-bit to 256-bit to fit Fernet algorithm keys.
2. We use this public key to encrypt the e-commerce requests among *M* and *TS*. Our protocol performs a strong encryption using high encryption randomness, which is difficult to crack when sent from *TS* to *M*.
3. The request information will be decrypted using the Fernet and ElGamal keys. Merchant / trust server get an decrypted text that is difficult to penetrate from attacker.
4. We use DLD technology to protect information, especially merchant information, from leakage in the process of creating keys, encryption and decryption processes.
5. Hiding information and security parameters on network devices, especially keys, is important in cases of hacking of these devices.

5.5.1 Key generation procedure

We use the ElGamal algorithm to generate public and private keys according to the following algorithm (1) steps:

1. We generate 1024-bit K_u public key and K_r private keys using parameters q and g were mentioned by ElGamal algorithm.
2. We divide the K_u public key into parts k_1, k_2, k_3, k_4 with a key size of 256 bits that fits the key size of the Fernet algorithm.
3. We perform XOR operations on keys such as $k_6 = k_3 \oplus k_4$, $k_5 = k_1 \oplus k_2$, then we get the final key, $FK=k_5 \oplus k_6$.
4. We add an ID to each key and perform the $FK_i = FK \oplus ID_i$ operation.
5. We use DLD to process the leakage probability (P_i) of a (s_i) data group from the guilty party to a group of agents (G_i).
6. We hide the keys a score(sco)$=PW \oplus K_r$ and $Fk_e = Fk_i \oplus sco \oplus PW$ In the case of the following connection, we do not generate keys, but we change the ID for each key

5.5.2 Encryption procedure

In a protocol we use pw, K_r, K_u and R_i (sell or push orders), but before we perform the encryption process the stored Kr and FK_i keys must be extracted as in Algorithm 2 from step 1 and 2. We extract the keys and then we perform the encryption operation using FK_i key, which is a Fernet 256 key and a random increase salt ($salt_i$) to provide more information security. Our protocol encrypts through $E_i = FK_i \,||\, R_i \,||salt_i$, then we use DLD This happens by leaking the ciphertext $P_i = E_i / s_i$ Then we compare the threshold (t) with the probability of leaking the ciphertext after it is sent over the network connection to the receiving end. We send encrypted text to the recipient and hide FK_i and K_r with FK_e, it is protected information that will be hard to hack.

5.5.3 Decryption procedure

It is a reverse process, an encryption process, public and private keys are used for decryption, and requests are decrypted when they reach the recipient. Our protocol decrypts the requests as in Algorithm (3), and we extract the keys from steps 1 and 2 up to $DR_i = Ei|| FK_i$, the decryption process is done, in our protocol we use DLD technology to find out the data leakage in the text after decoding and calculate the probability (P_i) and compare it with the threshold (t) and send the plain text of the requests to the receiver The plain text can be hidden using pw and we perform an XOR operation with the text $C_i = PW \oplus R_i$ stored in datasets for archiving. In the same way as Algorithm 2, Algorithm 3 stores keys anonymously.

Algorithm 1: Keys generation procedure *Input: q, g values and PW, t-threshold* *Output: K_r and K_u keys with 256-bit length* *1: Using ElGamal to generate K_u with 1024-bit length, K_r* *2: Dividing K_u to four parts with 256-bit length* *3: Four subkeys: k_1, k_2, k_3 and k_4* *4: Applying $\oplus$ with subkeys* *5: Obtaining FK with 256-bit length* *6-Adding ID for each key, Computing $FK_i = FK \oplus ID$* *7: Computing $P_i = G_i/s_i$* *8: if P_i (s_i) >t Declare as data leak* *9: else repeat step 7* *10: Protecting K_r and Fk_i on device* *11: Computing $sco = PW \oplus K_r$* *12: Storing $Fk_e = Fk_i \oplus sco \oplus PW$* *13: Next connection go to step 4 with changing ID order*	Algorithm 2: Encryption procedure *Input: K_r, K_u keys with 256-bit, PW and R_i, t-threshold* *Output: ER_i and P_i* *1: Extracting $K_r = PW \oplus sco$* *2: Extracting $Fk_i = Fk_e \oplus sco \oplus PW$* *3: Using Fk_i 256-bit with Fernet encryption* *5: Encrypting $E_i = R_i\|\|FK_i \| salt_i$* *6: $P_i = E_i / s_i$* *7: if P_i (E_i) > t Declare as data leak* *8: else repeat step 6* *9: Storing $Fk_e = Fk_i \oplus sco \oplus PW$* *10: Storing connection order on the sender side*

Algorithm 3: Decryption procedure *Input:* K_u *keys with 256-bit, PW and* E_i, *t-threshold* *Output:* DR_i, p_i *1: Extracting* $K_r = PW \oplus sco$ *2: Extracting* $Fk_i = Fk_e \oplus sco \oplus PW$ *3: Using* Fk_i *256-bit with Fernet decryption* *4: Using* $R_i = ER_i \| \| FK_i$ *5: Decrypting* DR_i *6:* $P_i = DR_i / s_i$ *7: if* $P_i (DR_i) > t$ *Declare as data leak* *8: else repeat step 6* *9: Saving* R_i *in dataset* *10: Storing* $C_i = R_i \oplus PW$ *11: Storing* $Fk_e = Fk_i \oplus sco \oplus PW$ *12: Storing connection order on the receiver side*	

6. Security and Performance of Proposed E-commerce applications

This section will discuss security analysis by testing the ability of our protocol to block e-commerce attacks, after that the SCYTHER tool is used to test the security of our protocol in practice.

6.1 Security analysis of a range of e-commerce attacks

6.1.1 Smishing

The attacker attempts to gain access to customer, merchant, organization, or company information in e-commerce applications such as merchant identities such as PIN, account and credit card details, personal information, and payment method in e-commerce transactions. In our protocol we use a public key K_u with each merchants ID which changes every time they connect. It's hard to hack information, we successfully fended off an attack.

6.1.2 Vishing

The intruder attempts to compromise information related to orders, sales, purchases, and payment processes while this information is being transmitted between customers, merchants, or another party. E-commerce transaction information is compromised and the attack is prevented by encrypting the data when it is sent. Using the Fernet algorithm and with a key of 256, it provides high security for hard-to-hack data.

6.1.3 Snooping

An unauthorized hacker or attacker tries to access the company's data, its institution, or a group of merchants and customers. Snooping involves monitoring a message sent through email or a program to remotely monitor activities on a network or host hacking a keylogger to capture data like password, username, address, etc. It also includes interception of data transmission and communication. Or an attack on an e-commerce server or an individual to collect information via network traffic for analysis. In our protocol, the keys K_u, K_r, and pw are hidden and inaccessible. This prevents the attacker from hacking.

6.1.4 Unfair evaluation attack

An attacker means the rater is intentionally harmful, the reputation worth of transactional partners in e-commerce is unfairly assessed, it also tries to penetrate the information of orders and information of merchants, such as the transaction number of the payment process, the time of delivery of goods, the quality of products and goods, and to protect this information, we have designed in our large protocol random keys, the size of bits is 1024 by Elgamal, and the information is encrypted using Fernet 256. This increases randomness and prevents the attacker hacked the information.

6.1.5 Collusive attack

The attacker tries to agree with many consumers or companies in order to raise prices, reduce production, or seize payment or buying and selling operations in a business, and tries to hack a password and keys designed for the system in the operations of electronic ordering commercial transactions. In our protocol, pw is not visible in the system, it is hidden, and the keys K_u, K_r are hidden. This prevents the attacker from hacking.

6.1.6 Pharming

The attacker penetrates the information of customers, merchants, companies, and transaction information, whether it is a purchase, sale, or payment in e-commerce applications, that is sensitive and important information by redirecting it to a fake website, companies, or customers by mistake. In our protocol, we use Fernet 256 encryption algorithm and DLD technology to protect data. This attack can be repelled.

6.1.7 Impersonalization

The hacker or attacker pretends to be another person or company and is socially constituted to obtain or collect information or gain access to a company, system or organization or hack information ordering sale, purchase and payment in electronic commerce applications or attacking the attack, in our protocol all keys are hidden K_u, K_r we encrypt information request with a random key of size 256.

This is difficult to crack the encryption and decryption process. It achieves high security requests and counteracts the attack.

6.1.8 Camera and Double Swipe method

The attacker tries to use the camera to capture the PIN or payment card, which is recorded when the customer enters the private PIN, and the merchant passes the card to the point of sale twice, the first at a fake point of sale and the other at a legitimate point, and credit cards are stolen in applications E-Commerce. To prevent any attack, in our protocol we use an asymmetric key through ElGamal algorithm which generates keys to increase the randomness K_r, K_u with an ID added to each key and is hidden for each transmission which is difficult to crack.

6.1.9 Dictionary attack

The intruder accesses the passwords in the dictionary to hack transaction information whether it is online purchase, sale or payment information. Frequent use of these words can guess a password, the decryption key in the pw protocol is unknown, it is difficult to know the K_u key, it is difficult to obtain keys with large random numbers based on the 1024 sentences algorithm, it also uses Fernet 256 encryption, decryption, and salt to increase the randomness and make data Safer can resist any attack.

Table 1: Comparison of attack prevention among Encryption algorithms.

Attack	[38] 2018	[36] 2020	[6] 2021	[33] 2021	[26] 2022	[34] 2022	[35] 2022	[3] 2022	[37] 2022	[39] 2022	[40] 2023	Proposed Protocol

Smishing									✔	✔	✔	✔
Vishing									✔	✔	✔	✔
										✔		✔
Snooping		✔		✔								✔
Unfair evaluation attack							✔					
							✔			✔		✔
									✔			✔
										✔		✔
collusive attack											✔	✔
		✔		✔							✔	
												✔
Pharming						✔						
										✔		
Impersonalization												
			✔		✔			✔				
Camera and Double Swipe method												
Dictionary attack												

6.2 Security Analysis Using SCYTHER

We introduce SCYTHER, a brand-new tool for verifying cryptographic protocols. The tool offers a variety of cutting-edge capabilities and is state-of-the-art in terms of verification speed. It can quickly verify the majority of protocols for an arbitrary number of sessions. All assaults discovered are actual attacks on the model since no approximation techniques are employed. New automatic protocol verification tool called Scyther. You can employ Scyther to look for attacks or carry out unrestricted verification. Scyther compares favorably to other protocol analysis tools for both objectives because it combines the best aspects of theorem proving or abstraction-based approaches (unbounded verification) and model checking methods (identifying attacks, termination). Additionally, Scyther includes a variety of innovative features that other tools do not have, like complete characterization and attack selection. Scyther has three different uses: as a command-line tool, as a backend for analysis programs using Python interface functions, or by using the graphical user interface. Scyther: Unlimited Check Security Protocols. Scyther uses the analysis of security requirements for a variety of protocols, detecting attacks on information, and verifying the confidentiality of this information, whether buying and selling operations, payment operations, or sending and receiving operations between a client, server, or merchant, or between companies or institutions, and verification Some of the information authentication through security requirements properties are Aliveness, Nisynch, Niagree, and Weakagree.

Description of Scyther with Proposed E-Commerce Protocol:

This tool uses to evaluate our suggested protocol, we used Security Protocol Description Language (SPDL) as in figure (5) where we use a set of commands between *M* merchant network entities and *TS* server machine, our proposed protocol is not attackable and is simulated between role events to communication between entities and check security requirements. They are Nisynch, Secret, Commitment, Niagree, and Alive. Scyther provides us with send () and rec () directives. The scyther tool can be used to find attacks and breaches can result from how the protocol is set up created. How is our protocol using requirements.

Secret: The results show that all parties are confidential and are not subjected to an attack, thus proving the privacy of the information.

ALive: The results display that the proposed protocol's transaction efficacy is available when needed. Commitment: is a specific data agreement, for example, in our proposed protocol *M* was agreed with *TS* on a combination of nonce T and R_i.

Niagree: A non-injectable guarantee of agreement is achieved by the proposed protocol. By doing so, the parties' message's integrity can be ensured.

Nisynch: The proposed protocol achieves non-injection synchronization guarantee to ensure that the protocol is against attack.

Scyther results : verify

Claim				Status		Comments
ElGamal_fernet	TS	ElGamal_fernet,TS1	Secret TSPW	Ok	Verified	No attacks.
		ElGamal_fernet,TS2	Secret XOR(TSPW,XOR(TSPW,TSKr))	Ok	Verified	No attacks.
		ElGamal_fernet,TS3	Secret KeysDivision(k1,k2,k3,k4)	Ok	Verified	No attacks.
		ElGamal_fernet,TS4	Secret XOR(XOR(k1,k2),XOR(k3,k4))	Ok	Verified	No attacks.
		ElGamal_fernet,TS5	Secret MKr	Ok	Verified	No attacks.
		ElGamal_fernet,TS6	Niagree	Ok	Verified	No attacks.
		ElGamal_fernet,TS7	Nisynch	Ok	Verified	No attacks.
		ElGamal_fernet,TS8	Alive	Ok	Verified	No attacks.
		ElGamal_fernet,TS9	Commit M,Er(Er(TSR,XOR(XOR(k1,k2),XOR(k3,k4))),Sal...	Ok	Verified	No attacks.
	M	ElGamal_fernet,M1	Secret MPW	Ok	Verified	No attacks.
		ElGamal_fernet,M2	Secret XOR(MPW,XOR(MPW,MKr))	Ok	Verified	No attacks.
		ElGamal_fernet,M3	Secret KeysDivision(k1,k2,k3,k4)	Ok	Verified	No attacks.
		ElGamal_fernet,M4	Secret XOR(XOR(XOR(XOR(XOR(XOR(k1,k2),XOR(k3,k4)),...	Ok	Verified	No attacks.
		ElGamal_fernet,M5	Secret XOR(TSPW,XOR(TSPW,TSKr))	Ok	Verified	No attacks.
		ElGamal_fernet,M7	Niagree	Ok	Verified	No attacks.
		ElGamal_fernet,M6	Nisynch	Ok	Verified	No attacks.
		ElGamal_fernet,M8	Alive	Ok	Verified	No attacks.
Done.		ElGamal_fernet,M9	Commit M,Concat(Er,Salti),t	Ok	Verified	No attacks.

Figure 5: Scyther security tool test of proposed e-commerce protocol.

Scyther Test Results:

Here we describe the e-commerce protocol test suggested by the Scyther tool. Figure (5) shows the test results of our protocol based on the immediate events 'Alive', 'Niagree', 'Nisynch', 'Secret' and 'Commit'. The test shows that public keys (TSK_u, Mk_u), private keys (TSK_r, MK_r), merchant requests, and service provider request (TSR/MR) are secret. It shows that orders are securely exchanged between network entities (*TS, M*) without any threats or attacks targeting network entities, security parameters, e-commerce orders sent and merchant data over the network. Our proposed protocol resists all attacks.

6.3 Results and discussion

The proposed protocol encryption algorithm was simulated using Java with a system Ubuntu 18.04.6 LTS. The computer used in the study has Windows 10 operating system and the processor is Intel (R) Core (TM) i5-2540M CP and it has 4.00 MB of RAM and Test the execution time encoding and decoding of the proposed algorithm, figure (6) shows the original Fernet algorithm the encryption time and decryption time, execution time lengths of decryption time. Figure (7) shows the time of encoding speed and time of decoding speed of the proposed algorithm. The proposed hybrid algorithm is Fernet and ElGamal. Each operation in its algorithm, whether it is the text encryption process or the decryption process, transforms the encrypted text into plain text, which is iterated 100 times. The slight difference in the encoding and decoding speed time depends on the size of the data each time. The results showed that the algorithm requires higher encryption time and lower decryption time, which leads to efficient performance of the algorithm compared to the original Fernet algorithm. Figures 8 and 9 show the performance of purchasing and payment orders by knowing the time of execution of requests and the time of decryption using the proposed algorithm, we note the time of execution of requests of lengths and depends on the volume of requests sent. Figure (10) shows the performance of the DLD technology using the proposed protocol by knowing the execution time of the decryption time for the keys, the encryption and decryption process, and the execution time for the encryption process is longer than the execution time for the decryption process, as well as the execution time for the keys, and depends on the size of the files. In our proposed protocol, we use DLD technology to detect data leakage and protect information, and a data breach or attack can occur. We use the ElGamal algorithm, it generates a key of size 1024, and we can use keys of different sizes and lengths 2048. Order information is exchanged between the merchant and the service provider in a single network, and it can be exchanged for a set of services across a set of networks.

As a result of merchants from all over the world relying on online transactions, e-commerce networks are enormous, which creates significant issues with the consumption of hardware/software and network resources like memory and execution time. Our protocol uses several lightweight methods that make it suitable for e-commerce applications. It relies on relatively small and random keys compared to other algorithms, which leads to reduced memory usage and consumption, especially in networks that use large enterprises and companies. Also, Fernet-256 encryption algorithm is fast when compared to encryption algorithms like DES, (RSA+AES(. In addition, our protocol relies on

DLD technology for data leak detection, the robust methodology used in designing our protocol makes it eligible for application in the e-commerce environment.

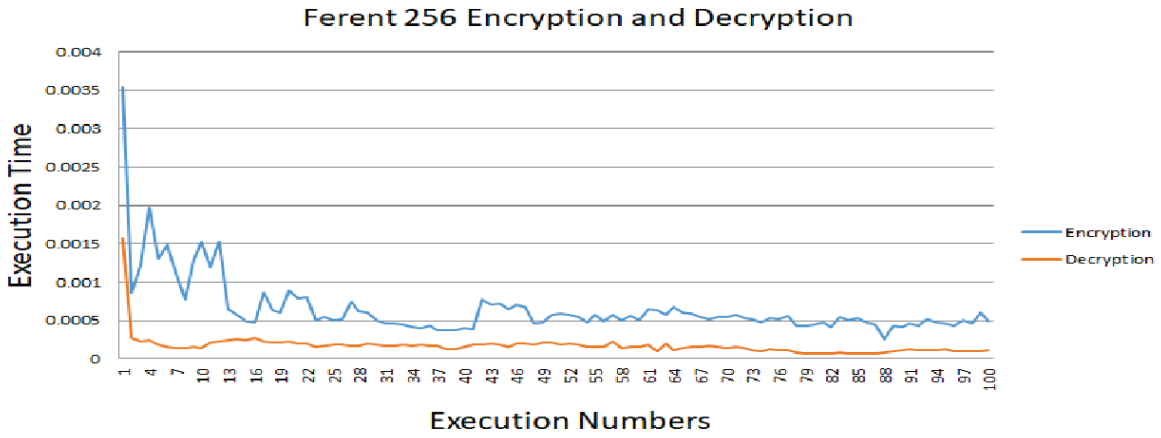

Figure 6 Encryption time and Decryption time Fernet 256.

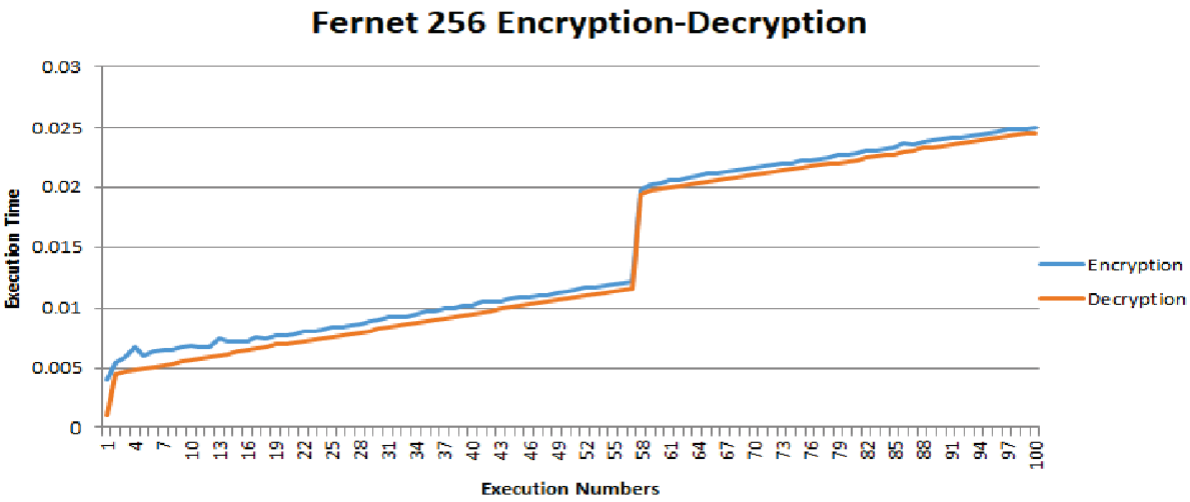

Figure 7 The Encryption time and Decryption time of the proposed algorithm.

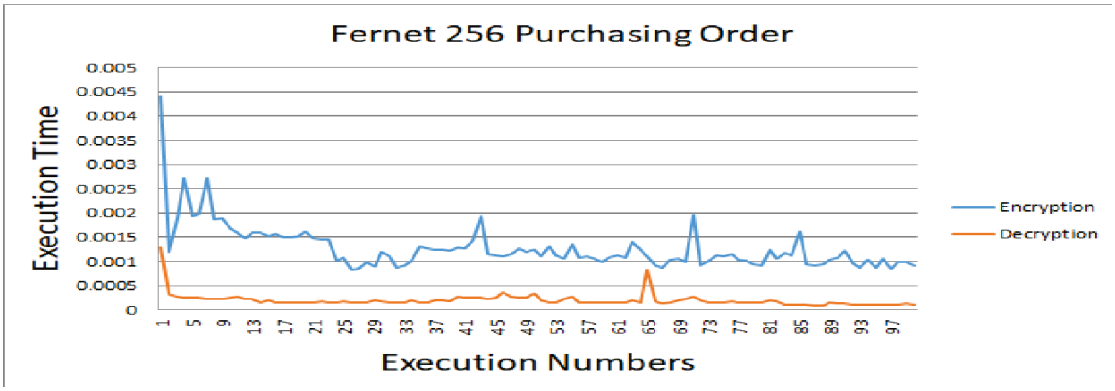

Figure 8 The Purchasing Order Encryption Time and Decryption Time.

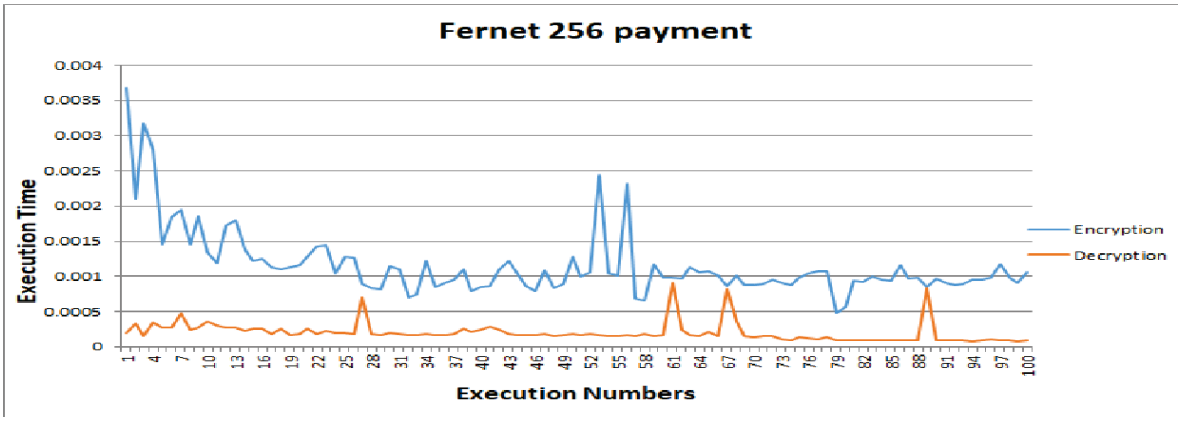

Figure 9 the Payment Encryption Time and Decryption Time.

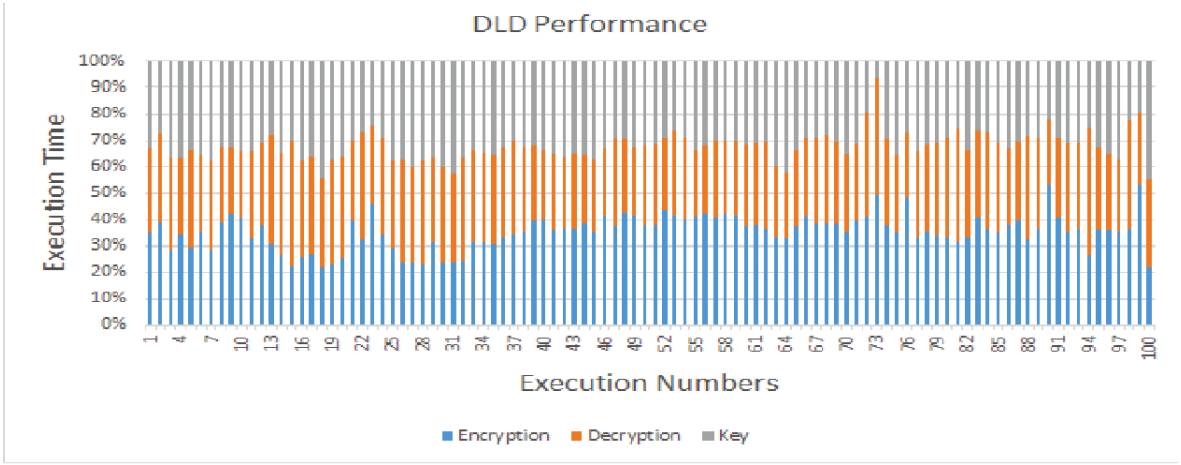

Figure 10 the DLD performance Encryption Time and Decryption Time and Key.

6. 4 Results Comparison and Analysis

In practice, our protocol performs lighter security measures for e-commerce applications than existing protocols. Although the environments, parameters and algorithms used in our protocol are not very identical to existing protocols, we investigated finding some comparable aspects between

our protocol and existing protocols. Table 2 provides a comparison of performance parameters (Encryption time, decryption time (between our protocol and existing protocols.

Awan et al. [41] used AES to encrypt data and scripts and find higher encryption and decryption execution time compared to our protocol providing better execution time. Al-gohany et al. [42] used DES to encrypt data in cloud computing with different file sizes. Encryption execution time is slow and decryption is faster, but compared to our protocol, it is less encryption and decryption time. Selvam et al. [43] Also used RSA and AES to encrypt the information of e-commerce applications. Encryption and decryption execution time uses AES and RSA. Compared with our protocols, we use the Fernet 256 algorithm to encrypt and decrypt, which leads to lightweight operations for merchant requests and less execution time. Sylfania et al. [44] also used of RSA and Blowfish to encrypt requests for e-commerce transactions using a hybrid algorithm, finding the time of executing requests and decrypting requests, compared to our protocol. The ElGamal algorithm is faster and more efficient than RSA. It does not use encryption and decryption, but rather generates random keys and a size of 256 that fits the size of the Fernet key achieves the best results.

Table 2 Comparison between the proposed cryptosystem, and existing protocols

Cryptosystem	Encryption	Decryption
AES [41]	0.1658	0.1789
Elgamal+ AES [12]	1,648	1,175
DES [42]	0.062	0.024
RSA+AES [43]	1.393	1.393
RSA+ Blowfish [44]	76.923	84.7826087
Proposed	0.00396248997	0.001015077

5. CONCLUSION

In e-commerce, transaction security is very important, online transaction security is a key task when it comes to deciding whether to buy a service or product online or to protect merchants' information, transaction information may be exposed to fraud that takes place online. We are currently designing a protocol that achieves high security for e-commerce transactions by using asymmetric keys such as the ElGamal algorithm and encryption technology that provides secure e-commerce transactions by using the fernet algorithm that achieves high data security and using DLD technology to protect information from leakage and piracy, and our protocol achieves high performance information and security from by countering attacks and achieving the best encryption speed of the proposed algorithm compared to the algorithms of previous studies. In future work, we provide higher security for e-commerce applications by combining the proposed algorithm with other algorithms such as RC4, Blowfish, and the use of random theories to increase randomness such as chaos theory.

REFERENCES

[1] **Asih, E. S., Nguyen, P. T., Lydia, E. L., Shankar, K., Hashim, W., & Maseleno**, A. (2019). Mobile E-commerce website for technology-based buying selling services.

[2] **Al-Ayed, S**. (2022). The impact of e-commerce drivers on e-customer loyalty: Evidence from KSA. International Journal of Data and Network Science, 6(1), 73-80.

[3] **Kumbhakar, D., Sanyal, K., & Karforma, S**. (2023). An optimal and efficient data security technique through crypto-stegano for E-commerce. Multimedia Tools and Applications, 1-14.

[4] **Jintcharadze, E., & Iavich, M**. (2020, September). Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems. In 2020 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-5). IEEE.

[5] **MALAU, H., & YOVIRA, V**. (2022). REVIEW OF TEXT BASED PASSWORD AND OTHER AUTHENTICATION METHODS FOR E-COMMERCE DATA PROTECTION. Journal of Theoretical and Applied Information Technology, 100(6).

[6] **Sidik, A. P., Efendi, S., & Suherman, S**. (2019, June). Improving One-Time Pad Algorithm on Shamir's Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012007). IOP Publishing.

[7] **Ali, G., Dida, M. A., & Elikana Sam, A.** (2021). A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. Future Internet, 13(12), 299.

[8] **Tyagi, S. S**. (2021). Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN). International Journal of Computer Networks and Applications, 8(4), 288-299.

[9] **Dong, Z.** (2021). Construction of mobile E-commerce platform and analysis of its impact on E-commerce logistics customer satisfaction. Complexity, 2021.

[10] **Abdul Hussien, F. T., Rahma, A. M. S., & Abdul Wahab, H. B.** (2021). A secure environment using a new lightweight AES encryption algorithm for e-commerce websites. Security and Communication Networks, 2021.

[11] **Kota, C**. (2022). Secure File Storage in Cloud Using Hybrid Cryptography. Available at SSRN 4209511.

[12] **Koppaka, A. K., & Lakshmi, V. N**. (2022). ElGamal algorithm with hyperchaotic sequence to enhance security of cloud data. International Journal of Pervasive Computing and Communications, (ahead-of-print).

[13] **Charles, V. B., Surendran, D., & SureshKumar, A**. (2022). Heart disease databased privacy preservation using enhanced ElGamal and ResNet classifier. Biomedical Signal Processing and Control, 71, 103185.

[14] **Ahmed, S., & Ahmed, T.** (2022). Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review.

[15] **Parvathi, R., Girish, M., Sandeep, M. G., & Abhiram, K**. (2022). Secured Blockchain Technology for Agriculture Food Supply Chain. Journal of Pharmaceutical Negative Results, 357-361.

[16] **Asmah, A., & Inayah, A. I**. (2023, January). Efficiency for E-Commerce Business Actors. In 3rd International Conference on Business Law and Local Wisdom in Tourism (ICBLT 2022) (pp. 185-193). Atlantis Press.

[17] **He, H., & Zhang, B**. (2023). Strategy Analysis of Multi-Agent Governance on the E-Commerce Platform. Journal of Theoretical and Applied Electronic Commerce Research, 18(1), 1-18.

[18] **Li, Z., Ren, L., Li, Z., Chen, J., Tian, X., & Zhang, Y**. (2023). Price Dispersion, Bargaining Power, and Consumers' Online Shopping Experience in e-Commerce: Evidence from Online Transactions. Mathematical Problems in Engineering, 2023.

[19] **Sugito, P**. (2023). Sales Multiplize Through E-Commerce Training for Batik Craftsman in Paiton Probolinggo. Empowerment Society, 6(1), 9-16.

[20] **De Feo, L., Poettering, B., & Sorniotti, A**. (2021, November). On the (in) security of ElGamal in OpenPGP. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 2066-2080).

[21] **Asri, R., Nasution, M. K., & Suherman, S**. (2019, June). Modification of chipper text Elgamal algorithm using split merge. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012054). IOP Publishing.

[22] **Sari, P. P., Nababan, E. B., & Zarlis, M**. (2020, June). Comparative study of luc, elgamal and RAS algorithms in encoding texts. In 2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT) (pp. 148-151). IEEE.

[23] **Arboleda, E. R**. (2019). Secure and fast chaotic Elgamal cryptosystem. Int. J. Eng. Adv. Technol, 8(5), 1693-1699.

[24] **Harjito, B., Setyowati, T., & Wijayanto, A**. (2022). Comparative Analysis between Elgamal and NTRU Algorithms and their implementation of Digital Signature for Electronic Certificate. International journal of electrical and computer engineering systems, 13(9), 729-739.

[25] **Ismail, E. G., CHAHBOUN, A., & RAISSOUNI, N**. (2020). FERNET SYMMETRIC ENCRYPTION METHOD to GATHER MQTT E2E SECURE COMMUNICATIONS for IoT DEVICES.

[26] **Prashanth, C., Teja, D. B. S., & Lavanya, V**. (2022). Securing the Data in Cloud Using Fernet Technique (No. 9237). EasyChair.

[27] **Habibu, T., Luhanga, E. T., & Sam, A. E**. (2019). Developing an algorithm for securing the biometric data template in the database.

[28] **Singh, A., Ikuesan, R. A., & Venter, H**. (2022). Secure Storage Model for Digital Forensic Readiness. IEEE Access, 10, 19469-19480.

[29] **Gupta, I., & Singh, A. K**. (2022). A Holistic View on Data Protection for Sharing, Communicating, and Computing Environments: Taxonomy and Future Directions. arXiv preprint arXiv:2202.11965.

[30] **Patil, R. C., Kumar, A., Narmadha, T., Suganthi, M., Rao, A. V. S. R., & Rajesh, A**. (2022). Data Leakage Detection in Cloud Computing Environment Using Classification Based on Deep Learning Architectures. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 281-285.

[31] **Verma, R., Gautam, V., Yadav, C. P., Gupta, I., & Singh, A. K**. (2020, May). A Survey on Data Leakage Detection and Prevention. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[32] **https://www.wordtemplatesonline.net/payment-receipt-templates/free e-commerce form**.

[33] **Badotra, S., & Sundas, A**. (2021). A systematic review on security of E-commerce systems. International Journal of Applied Science and Engineering, 18(2), 1-19.

[34] **Alqassab, A., & Hikmat Ismael, Y**. (2022). EMV Electronic Payment System and its Attacks: A Review. AL-Rafidain Journal of Computer Sciences and Mathematics, 16(1), 23-29.

[35] **Xiao, Y., Zhou, C., Guo, X., Song, Y., & Chen, C**. (2022). A Novel Decentralized E-Commerce Transaction System Based on Blockchain. Applied Sciences, 12(12), 5770.

[36] **Kaushik, D., Gupta, A., & Gupta, S**. (2020, May). E-commerce security challenges: A review. In Proceedings of the international conference on innovative computing & communications (ICICC).

[37] **Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S**. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology, 13, 4863.

[38] **Odunze, D**. (2018). Cyber victimization by hackers: A criminological analysis. Public Policy and Administration Research, 8(01), 08-15.

[39] **Roy, S., Sharmin, N., Acosta, J. C., Kiekintveld, C., & Laszka, A**. (2022). Survey and taxonomy of adversarial reconnaissance techniques. ACM Computing Surveys, 55(6), 1-38.

[40] **Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J.** (2023). Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. Sensors, 23(6), 3155.

[41] **Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A**. (2020). Secure framework enhancing AES algorithm in cloud computing. Security and communication networks, 2020, 1-16.

[42] **Al-gohany, N. A., & Almotairi, S**. (2019). Comparative study of database security in cloud computing using AES and DES encryption algorithms. Journal of Information Security and Cybercrimes Research, 2(1), 102-109.

[43] **Devassy, N.** (2023). Research Project Questions (Doctoral dissertation, Dublin, National College of Ireland).

[44] **SYLFANIA, D. Y., JUNIAWAN, F. P., & PRADANA, H. A.** (2020, May). Blowfish–RSA Comparison Analysis of the Encrypt Decrypt Process in Android-Based Email Application. In Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019) (pp. 113-119). Atlantis Press.