A Fair Exchange & Customer Anonymity Protocol Using A Trusted Third Party for Electronic Commerce Transactions & Payments

Fahad A Alqahtani

Software Technology Research Laboratory (STRL)
De Montfort University, Leicester, United Kingdom

ABSTRACT

The rapid development of technology and the reach of such technologies at affordable costs has made it possible for all people across the world to make purchases at a click of the mouse and at their convenience.Electronic commerce technologies and protocols facilitate the processing of online transactions. Trust plays a major role in e-commerce transactions and various protocols help establishing this trust by providing fair exchange and anonymity.

The research aims at designing and developing a protocol that provides both fair exchange and anonymity, thus avoiding the need to have manual dispute resolution. It takes into account the technical flaws researched and overcomes those by implementing methods to ensure that confidentiality and integrity of the messages are maintained by making sure that the Trusted Third Party does not have the authority to view or modify the messages but can only verify the authenticity of the other two parties.

KEYWORDS

E-commerce, Trust, fair exchange, anonymity, trusted third party, security

1.0 INTRODUCTION

The rapid development of technology and the reach of such technologies at affordable costs has made it possible for all people across the world to make purchases at a click of the mouse and at their most convenient time. Electronic commerce technologies and protocols facilitate the processing of online transactions. The development of these technologies has led to more and more merchants being able to sell their goods online.

However, complications arise due to the fact that both transacting parties namely the merchant and the customer could be anybody and this could lead to issues of trust and security. Customer is not very sure whether he/she would be able to get the goods that he/she has ordered for and hence there is an issue of trust involved here. From the point of view of the merchant, he is taking a risk by sending goods and awaiting payment from the customer.

It also poses a lot of questions such as: How do I trust that the goods that I ordered would definitely reach me? Or what happens if I cancel the transaction, would I be wrongly charged? Or how will my online identity be protected and how secure are my personal details that I have given while registering with the website? The customer is worried about protection of online identity so that in the future he/she is not bombarded with spam or identity theft. Since most payments are

traceable, customers are also worried about the merchants tracking their purchasing habits thus causing privacy issues.

The party that sends the information, goods and/or money first is at a greater risk as the party in receipt could abort the transaction and receive the goods but not pay – in simpler terms misbehave. This poses a lot of questions about fairness. The main aim of this research is to propose a protocol that ensures fairness during transactions while making sure that the identities of the customers remain a secret (anonymity) to ensure privacy of the customer.

Thus the main idea of the research is to propose an electronic commerce protocol which will ensure that both the transacting parties remain honest while enabling efficient and smooth exchange of information (including payment related information), digital goods and/or services online and also keeping the identity of the customer secret.

1.1 MOTIVATION

Anonymity and Fair Exchange plays a pivotal role in the provision of trust. Though there are many protocols in the literature that concentrate on Fair Exchange [1][2][3][4][5][6][7][8][9] only a very few of these protocols concentrate on both anonymity and fair exchange aspects [4][6][9].

Though these three protocols provide fairness & anonymity there are various weaknesses that are inherent. One for example is the number of messages and also the fact that the TTP is not entirely trustworthy as the TTP is capable of being able to view and/or modify the message. Though these protocols ensure that the TTP does not collude, these does not guarantee that the TTP would not masquerade. Also it does not provide any mechanism to tackle a situation where the TTP modifies the message thus becoming semi-trusted.

1. The research aims at designing and developing a protocol that provides both true fair exchange and anonymity, thus avoiding the need to have manual dispute resolution techniques. It takes into account the technical flaws researched and overcomes those by implementing methods to ensure that confidentiality and integrity of the messages exchanged between the merchant and the customer are maintained by making sure that the Trusted Third Party (TTP) does not have the authority to view or modify the messages but can only verify the authenticity of the other two parties. This is done to make sure that the TTP totally trusted.
2. The research aims at implementing a prototype for the proposed protocol, thoroughly evaluating it against different criteria and model checking the protocol to ensure the logic is correct and validating the protocol to make sure that the core functionality proposed by the protocol holds good and that it satisfies all the key properties. The research proposes to implement the protocol in order to ensure that the designed protocol is ready for the real-world and to prove that it is not just a research-based, theoretical design but a robust, fully deployable model.

The central research question is to develop and design an electronic commerce protocol that would provide the following features:

- Fair exchange through all the phases of the electronic commerce transaction
- Total customer anonymity
- Entirely Trustworthy Trusted Third Party (TTP)
- Built-in dispute resolution mechanism
- Termination of the protocol when either parties become dishonest
- Efficient and effective buy not cumbersome (with limited number of messages).

2.0 IMPOSING FAIRNESS & ANONYMITY PROTOCOL

The chapter begins with the approach the protocol takes and the underlying evolution concept of the protocol followed by a detailed explanation of the Imposing Fairness & Anonymity (IFA) protocol where it is discussed and analysed to see if the protocol satisfies the criteria of fairness and anonymity.

2.1 RESEARCH PROBLEM AND REQUIREMENTS

The main objective of this research is to propose an efficient and effective protocol for electronic commerce transactions that provide both anonymity and fair exchange. The protocol is based on three other protocols that provide the same features namely Ray et al'sanonymous and failure resilient fair-exchange electronic commerce protocol, Zhang et al'sEfficient Protocol for Anonymous and Fair Exchange and . Though these protocols have achieved both the above mentioned characteristics of anonymity and fair exchange, there are inherent problems that these protocols have as discussed in the earlier chapters. The protocol also makes use of an online Trusted Third Party to mediate between the transacting parties and also for any dispute resolution purposes. The protocol is also aims at providing fair exchange throughout all phases of an electronic commerce transaction.

2.2 NOTATIONS AND PARTICIPANTS

This section of the document aims at describing the key participants or entities in the proposed electronic commerce protocol and how these participants are denoted. It also aims at describing briefly the role each participant plays in the proposed electronic commerce protocol.

1. Merchant: Merchants are entities (individual or corporate) that have digital products to sell. Merchant is represented by the letter M.
2. Customer: Customers are entities (individual or corporate) that require digital products sold by the merchant. In the protocol, Customer is represented by the letter C.
3. Bank: Helps withdrawal and redemption of electronic cash to the Merchant and Customer. In the protocol, Bank is represented by the letter B.
4. Trusted Third Party: Refers to an individual or corporate that helps mediating the electronic commerce transaction. It is an entity trusted by both the Customer and the Merchant. In the protocol, it is represented as TTP.
5. Certificate Authority: Refers to an individual or corporate that is responsible for issuing, verifying and revoking certificates and is represented in the protocol as CA.
6. Producer: Producers are entities (individual or corporate) that create and own digital contents and have the digital copyrights over the products. In the protocol, Producer is represented by the letter P.

2.2.1 PROTOCOL ASSUMPTIONS

The proposed electronic commerce protocol assumes the following and aims at achieving fair exchange and customer anonymity. First and foremost, the protocol assumes that a secure communication channel has already been established and will continue to remain secure throughout the electronic commerce transaction. Hence it does not deal with Transport Layer Security. Secondly, the protocol does not dictate who the Trusted Third Party would be. It assumes that the customer and the merchant would have mutually agreed on who the TTP would be and hence not be involved in the selection process.

The other assumptions include:

1. The trusted third party (TTP) is semi-trusted and hence is used only to validate the authenticity of the merchant to the customer and vice-versa. It therefore makes use of TTP heavily in the initial stages while trust is being established.
2. The Trusted Third Party (TTP) cannot read or modify messages sent.
3. The Trusted Third Party will not collude with any other party
4. All parties involved in the protocol will behave rationally
5. The protocol would avoid any replay attacks by making use of cryptographic mechanism such as Digital signature and the messages are time stamped. Time stamps can also be made use in case of dispute resolution.
6. The protocol also assumes that a resilient connection is present between all parties involved namely the customer, merchant and the Trusted Third Party. This means that all messages that are sent are relayed appropriately to the appropriate recipients.
7. With regards to payment, the protocol makes use of digital cash and any double payment is are dealt with and refunded to the customer by the appropriate payment authority.
8. The protocol also assumes that all the transacting parties make use of the same cryptographic mechanisms for all purposes including encryption, decryption, signing messages and hashing.

2.3 PROTOCOL PROCESS

This section of the document aims at providing a gist of the steps involved in the protocol. In summary, the following are the key stages in the proposed protocol. It describes the messages sent between all parties involved in the protocol process.

Step 1: The merchant gets approval to sell the digital contents from the producer (P), who owns the digital copyrights for the product
Step 2: The merchant, on receiving the go ahead from the producer to sell the products, now gets the digital contents verified by a certificateauthority (CA). The CA verifies the identity of the merchant and issues a certificate that is digitally signed.
Step 3: The merchant uploads the product details online to his website to attract potential customers. Along with the product details, the merchant also uploadsthe certificate received by the certification authority to help enhance the perception of trust.
Step 4: The interested customer now views the product and verifies the digital signature and gets to understand the authenticity of the merchant.
Step 5: The customer withdraws cash (electronic cash) from the bank.
Step 6: The bank issues the electronic cash to the customer
Step 7: The customer, after viewing the digital products available for purchase contacts the Trusted Third Party (TTP) with a hashed, time-stamped andencrypted Electronic Cash. It is encrypted to ensure that the TTP cannot read it, time-stamped to avoid any replay attacks and hashed to protect the integrity of the file and avoid any file tampering.
Step 8: The Trusted Third Party (TTP) verifies the hash and now sends the same to the merchant. This allows the merchant to trust that the customer is indeed genuine and will definitely pay on receipt of products being delivered.
Step 9: The merchant now contacts the Trusted Third Party (TTP) with hashed,time-stamped and encrypted digital product. The product is encrypted to avoid any misuse by intruders or the Trusted Third Party and hashed to be able to verify if tampered.
Step 10: The Third party now verifies this and sends the same to the Customer
Step 11: Merchant and the customer now directly send each other thehash to verify.
Step 12: Each of them verify the hash individually and exchange private keys
Step 13: Merchant requests the Trusted Third Party to send the electronic cash that the customer

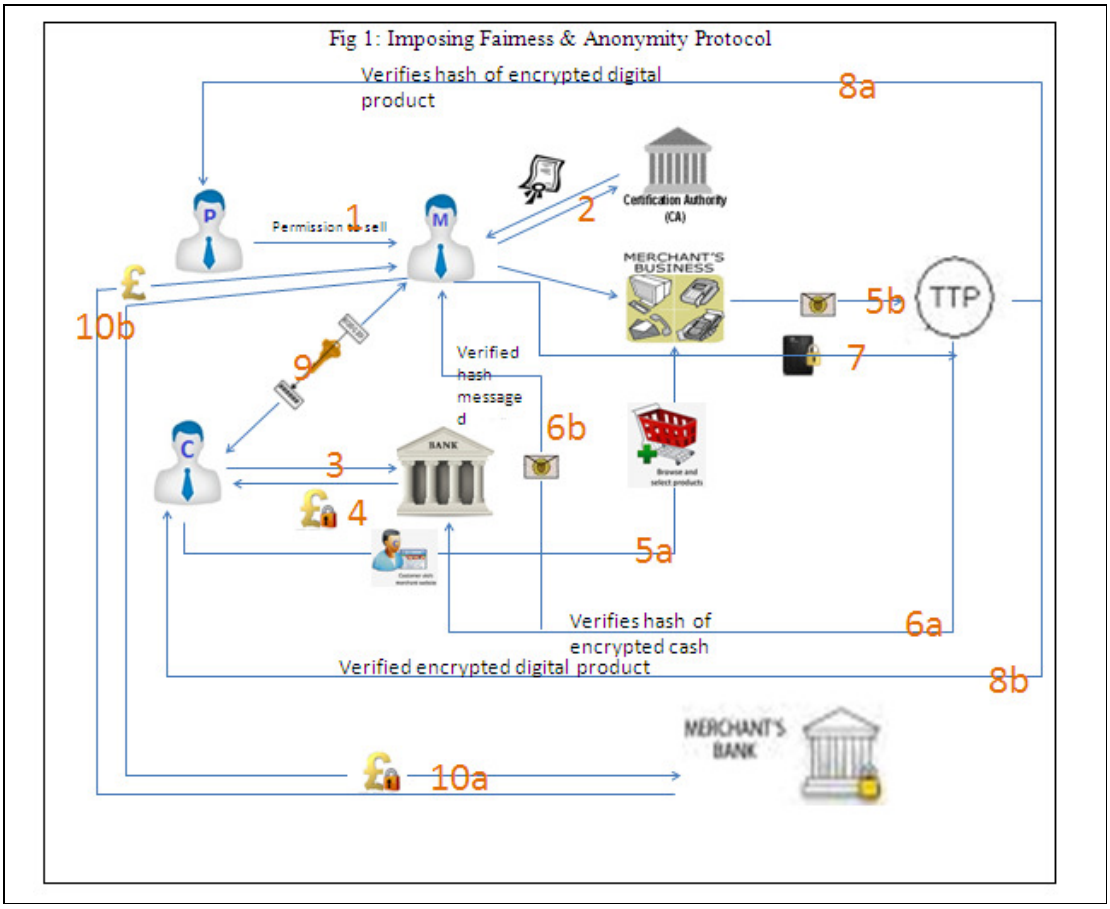
sent earlier.

Step 14: The Trusted Third Party sends the encrypted cash to the merchant whothen decrypts the same using the key exchanged in step 12

Step 15: The Customer requests the Third Party to send the digital productthat the merchant sent

Step 16: The Trusted Third Party sends the encrypted product to the customerwho then decrypts using the keys exchanged in step 12

Step 17: Merchant sends request to the bank to redeem the cash



2.4 PROTOCOL ANALYSIS

The aim of this section is to analyse the protocol proposed in order to be able to identify any flaws in the protocol and also to be able to justify the properties that the protocol aims at achieving. This section not only aims at identifying the gaps in the protocol but also see if the proposed protocol is able to overcome the drawbacks mentioned in the other protocols discussed earlier. It also discusses the possibilities when there are might be disputes and how the protocol enables the transacting parties to resolve these conflicts.

2.4.1 FAIR EXCHANGE

One of the key desirable properties that the proposed protocol aims at providing is fair exchange. This section aims at analysing in detail this property of the protocol. The Bank (B) is entirely trustworthy just like the Certificate Authority (CA). The Trusted Third Party is semi-trusted and is capable of masquerading. The other two parties namely the Customer (C) and Merchant (M)

are very much capable of misbehaving and being dishonest. This section shows a case by case scenario of all possible actions that are considered dishonest. The below sections give an even more detailed analysis that help identify dishonesty amongst the participants.

Scenario 1: The Merchant (M) sends a different price to the Customer (C). This inconsistency would be easily detected by the Customer, when the Customer checks the product price received to the original product price when he/she was browsing the Merchant's website.
Scenario 2: The Merchant (M) sends a different product to the Customer (C). This inconsistency is again easily detected by the Customer when the Customer checks the Hash of the message.
Scenario 3: The Merchant (M) tries to redeem cash from the Bank before sending the digital product. This is not possible as the Customer would not exchange the decryption key for the electronic cash sent to enable the Merchant decrypt the message to redeem cash from the Bank (B).
Scenario 4: The Customer (C) sends no cash. This is identified as the decryption key for the digital product sent by the Merchant (M) would not be exchanged with the customer to enable decryption of the message and usage of the product.
Scenario 5: The Customer (C) sends wrong amount. This inconsistency is identified by the Merchant when he checks with the Bank (B) to verify funds of the Customer (C).
Scenario 6: The Third Party modifies the message sent by the Merchant. This is easily identified by the Customer (C) as the hash of the message would not match.
Scenario 7: The Third Party modifies the message sent by the Customer. This is easily identified by the Merchant (M) as the hash of the message would not match.
Scenario 8: The Third Party does not forward the digital product to the Customer or the electronic cash to the Merchant. This is rendered useless as the Customer (C) and the Merchant (M) exchange the decryption keys in private without involvement of the trusted third party. Without the key, the trusted third party cannot do anything with these messages.
Scenario 9: The customer, after sending the electronic cash but before receiving the digital product decides to withdraw from the transaction. This is managed easily as the customer can refrain from exchanging the decryption key with the Merchant (M). Without the decryption key the electronic cash sent would be rendered useless.
Scenario 10: The merchant, for some reason, after sending the digital product to the Trusted third party but before receiving the electronic cash decides to not proceed with the transaction. This again is easily managed as the Merchant can refrain from exchanging the decryption key with the Customer (C). Without the decryption key, the customer cannot access or make use of the digital product.

2.4.2 ANONYMITY

The protocol's another key feature is provision of customer anonymity. This property is achieved by two means:

1. Usage of anonymous electronic channels
2. Usage of anonymous electronic cash

In the protocol, during the second phase (the negotiation phase), the Merchant (M) or the trusted third party are not aware of the true identity of the Customer (C) as the customer does not share this.

In the next phase (the withdrawal phase), only the Bank (B) is aware of the Customer's (C) true identity as the Customer would have shared this information with the Bank earlier. However, this does not compromise the anonymity of the Customer as the Bank cannot communicate this real identity of the Customer (C) in any other phase to any other parties involved due the usage of the Blind Signature Concept.

Similarly, in the purchase phase no other participant including the Trusted Third Party is aware of the Customer's identity as the Customer (C) does not share any personal details. Since anonymous electronic cash is used for the transaction, which makes it impossible to trace back to the Customer's real identity.

In the arbitration phase again, the Customer (C) does not share any details regarding his true identity and hence no other party involved would be able to identify the true identity of the Customer.

Thus, under all circumstances, no other participant, except the Customer would be able to find out the true identity of the Customer. From the above, it is clear that the Customer's identity is protected during all phases of the electronic commerce transaction. Thus the proposed protocol provides complete anonymity to the Customer (C).

2.4.3 PAYMENT SECURITY

One of the other key features that the protocol assured was security of payment. Like traditional commerce, there is always a threat to the security of payment in case of electronic commerce. However, unlike traditional commerce, payment security has additional challenges that are so much varied.

Key researchers in this area of payment security discusses two key challenges (Xue et al, 2005; D Chaum, 1983; Lin et al, 2006). These key factors include:

1. Prevention of forging electronic cash and
2. Double-Spending of electronic cash

This section of the document aims at highlighting various scenarios that where the transacting parties try to either double-spend the electronic cash or forge electronic cash and also describes in detail what happens when such attempts are being made.

Scenario 1: The Customer (C) tries to forge the electronic cash to gain benefit that is not legal from the Bank (B)

Result: This is not possible. In order to generate electronic cash (or forge it), the Bank's signature is required. For obtaining the signature of the Bank, it is necessary for the Customer to know the Bank's Private Key. Therefore, if the Customer (C) tries to forge any other values in the electronic cash, the Bank would be able to easily identify the anomaly.

Scenario 2: The Merchant (M) tries to modify the electronic cash received from the Customer (C) before sending it to the Bank (B) in order to gain benefit that he/she is not legally entitled to gain.

Result: This is not possible. In order to make modifications to the electronic cash (or forge it), it is necessary that the Merchant has the Bank's signature. To forge the electronic signature itself, it is necessary for the Merchant to have knowledge of the Bank's Private Key that would be used for signing the electronic cash it generates. Since this is the private key, the Merchant would never be able to get access of this. Hence, any attempt made by the Merchant (M) to forge the value of the electronic cash would be easily identified by the Bank.

Scenario 3: The Customer (C) tries to use spent electronic cash (electronic cash that has been spent on an earlier transaction or purchase) to buy a digital product from the Merchant (M).

Result: This again is not possible. Every time the Customer spends electronic cash, the Bank enters the details of the spent cash in its Database. When a customer thus sends electronic cash, the Bank would decrypt the message, compare the kept cash with the spent cash and if the message sent is already stored in the spent cash database, the bank easily identifies the anomaly.

From the above scenarios, it can be clearly understood that neither of the transacting parties namely the Customer or the Merchant can forge the electronic cash. It can thus be said that the protocol offers good payment security.

2.4.4 DISPUTE RESOLUTION

At the end of an electronic commerce transaction, just like a traditional commerce transaction there might be disputes that need to be resolved. Unlike traditional commerce, however, the disputes are varied in nature and dispute handling and resolution is a lot different in an electronic commerce scenario.

With specific reference to the proposed Imposing Fairness and Anonymity protocol, after the completion of the transaction between the Merchant (M) and Customer (C), there are four different scenarios that are likely to occur from the point of view of the Customer (C). These scenarios are as follows:

1. Customer receiving the correct digital products that he/she ordered for
2. Customer did not receive the correct digital products
3. Customer received the correct digital products but the product(s) were defective or not according to the specification
4. Customer did not receive the product at all

The protocol aims at achieving the first output and that is the most desired outcome of the protocol, which is smooth facilitation of the transaction and guaranteeing fair exchange.
Similarly, from the point of view of the Merchant (M), there are three key outcomes that are most likely to occur. These outcomes are as follows:

1. The Merchant receiving the correct payment for the digital product(s) sold.
2. The Merchant receiving incorrect payment for the digital product(s) sold.
3. The Merchant not receiving the payment for the digital product(s) sold.

Again, the protocol aims at achieving the first outcome as that is the most desired one. If however, for any reason the second or the third output occurs, then there is a dispute. Incorrect product refers to the digital product that was not requested by the customer or more specifically a product that does not match the product description given by the merchant. Similarly, incorrect payment refers to the sum of money that does not match the Merchant's price mentioned or more specifically payment that is not exactly what the Merchant advertised and requested. In such cases, dispute resolution plays a major role in identifying the cause of the dispute and provides a means to resolve the issue.

The aim of this sub-section is to discuss in detail the various possibilities that might arise at the end of the electronic commerce transaction and points out to scenarios where there might be issues or disputes. The protocol, however, does not involve or discuss about the mechanism that needs to be used or the steps to be followed when there is a dispute. It is assumed that the aggrieved party in the transaction will take appropriate measures in order to be indemnified.

Customer	Merchant	Outcome
Receive the correct product	Receive the correct payment	No Dispute
Receive the correct product	Receive incorrect payment	Dispute raised by the Merchant
Receive the correct product	Does not receive the payment	Dispute raised by the Merchant
Receive incorrect product	Receive correct payment	Dispute raised by the Customer
Receive incorrect product	Receive incorrect payment	Dispute raised either by the customer or the merchant
Receive incorrect product	Does not receive the payment	Dispute raised either by the customer or the merchant
Receive correct product but defective	Receive correct payment	Dispute raised by the customer
Receive correct product but defective	Receive incorrect payment	Dispute raised either by the customer or the merchant
Receive correct product but defective	Does not receive the payment	Dispute raised either by the customer or the merchant

As seen above, there are totally twelve possibilities where the dispute might arise. From the above table it can be noted that if both the parties the customer and the merchant receive the products then there is no dispute.

Similarly, during the electronic commerce transaction, there are various possibilities where disputes might occur. The below table identifies the possibilities where the transacting parties might be dishonest and the scenarios which might lead to a dispute.

2.4.5 DETECTION OF DISHONESTY

For the protocol to be able to implement fair exchange, it is pivotal that the protocol is able to identify behaviours of dishonesty. It is very important that the protocol enables either of the transacting parties to detect any kind of abnormal behaviours that are being displayed by the other. The customer can act in a dishonest manner by doing the following:

1. Sending incorrect payment
2. Payment that is encrypted with a different key than the one exchanged with the Merchant (M)
3. Invalid signature on the payment

When the Merchant receives the payment details from the Trusted Third Party, M will check the signature on the payment along with the encryption key. If the encryption key is different to the one that's being exchanged, the customer's dishonesty is clearly shown.

Similarly, the merchant can act in a dishonest manner by doing the following:

1. Sending incorrect product
2. Encrypting the product with a different key than the one exchanged with the Customer (C)
3. Invalid signature on the product

Similar to the above, when the customer receives the product details from the Trusted Third Party, C will check the signature on the product along with the encryption key. If the encryption key is different to the one that's being exchanged, the Merchant's dishonesty is clearly shown.
In worst case scenarios, there is also a possibility that the Trusted Third Party acts as an intruder and masquerades. The Trusted third party can also in some cases modify the messages sent to the customer and/or the merchant. The dishonesty that could be detected by the protocol is as follows:

1. Modifying message
2. Replaying the stored message
3. Not sending the product and/or the cash to the designated party

If the message is modified by the Trusted Third Party, the hash value of the message changes and hence the Customer (C) or the Merchant (M) can easily detect the interception. The messages are time-stamped and hence it makes it easy to check the time when the message was originally sent and either of the parties can detect any dishonesty in the Trusted Third Party and reject the messages if the time frame has elapsed. The Trusted Third Party, can sometimes become dishonest and not send the products and or cash to the appropriate, designated party. In this case, it will not be of any use as the Merchant (M) and the Customer (C) alone has the decryption key that they have shared in private. Hence, even though the TTP has the product/cash, it would be of no use as the TTP cannot decrypt the same without the shared key.
If either the Customer (C) or the Merchant (M) does not send the product/cash, the protocol automatically terminates as both of them sends it to the TTP and the Trusted third party would only send the cash to the Merchant (M) and product to the customer (C) only after receipt of both the items. Hence, the trustworthy party will not be disadvantaged by having sent the product and/or cash.

Thus the four possibilities for the Merchant with reference to the product and encryption key are:

1. Merchant sends the correct product and the right encryption key. This is the perfect situation and proves that the Merchant (M) is honest.
2. Merchant sends the correct digital product but the wrong decryption key. This implies that the Merchant (M) is dishonest.
3. Merchant sends the incorrect digital product (faulty or the wrong product) and the incorrect decryption key. This again shows that the Merchant is dishonest.
4. The Merchant sends the wrong digital product and the correct decryption key which indicates that the merchant is dishonest.
5.

The table below explains the possibilities for the Merchant

Product	Decryption Key	Result
√	√	Honest
√	X	Dishonest
X	X	Dishonest
X	√	Dishonest

With reference to the encryption key and cash, there are again four different possibilities that exist for the Customer (C) with specific reference to electronic cash and hash value. This includes the following:

1. Customer sends the correct cash and the right encryption key. This is the perfect situation and proves that the Customer (C) is honest.
2. Customer sends the correct electronic cash but the wrong decryption key. This implies that the Customer (C) is dishonest.
3. Customer sends the incorrect electronic cash (wrong amount) and the incorrect decryption key. This again shows that the Customer is dishonest.
4. The Customer sends the wrong electronic cash and the correct decryption key which indicates that the Customer is dishonest.

5.

The table below explains the possibilities for the Customer

Electronic Cash	Decryption Key	Result
√	√	Honest
√	X	Dishonest
X	X	Dishonest
X	√	Dishonest

There are four possibilities for the Merchant with reference to the product and the digital signature. These are:

1. Merchant sends the correct product and the right digital signature. This is the perfect situation and proves that the Merchant (M) is honest.
2. Merchant sends the correct digital product but the wrong digital signature. This implies that the Merchant (M) is dishonest.
3. Merchant sends the incorrect digital product (faulty or the wrong product) and the incorrect digital signature. This again shows that the Merchant is dishonest.
4. The Merchant sends the wrong digital product and the correct digital signature which indicates that the merchant is dishonest.

The table below explains the possibilities for the Merchant

Product	Digital Signature	Result
√	√	Honest
√	X	Dishonest
X	X	Dishonest
X	√	Dishonest

Similarly, there are four possibilities for the Merchant with reference to the product and the digital signature. These are:

1. Customer sends the correct electronic cash and the right digital signature. This is the perfect situation and proves that the Customer (C) is honest.
2. Customer sends the correct electronic cash but the wrong digital signature. This implies that the Customer (C) is dishonest.
3. Customer sends the incorrect electronic cash (wrong amount) and the incorrect digital signature. This again shows that the Customer (C) is dishonest.
4. The Customer sends the wrong electronic cash and the correct digital signature which indicates that the merchant is dishonest.

The table below explains the possibilities for the Customer

Electronic Cash	Digital Signature	Result
√	√	Honest
√	X	Dishonest
X	X	Dishonest
X	√	Dishonest

2.4.6 Scenario Analysis

This section aims at performing a scenario analysis. Various scenarios that might take place where the transacting parties are either honest or dishonest are taken into consideration and the execution of the protocol is checked.

The various scenarios where either party could behave in a dishonest manner are shown in the table below

Customer (C)	Merchant (M)	Result
Honest	Honest	Normal
Honest	Dishonest	Abnormal
Dishonest	Honest	Abnormal
Dishonest	Dishonest	Abnormal

We have now analysed what happens when either of the parties are dishonest. The next step is to analyse what happens when either of the parties wish to withdraw. Here, we are assuming that the first step of sending the electronic cash or the digital product to the trusted third party as already occurred and the Customer or Merchant at this stage wishes to withdraw. The following table describes all the scenarios relating to this:

Customer	Merchant	Result
Sends the electronic cash to the TTP and wants to continue	Sends the digital product to the TTP and wants to continue	Protocol proceeds in the normal flow
Sends the electronic cash to the TTP and wants to continue	Sends the digital product to the TTP but wants to withdraw	Protocol terminates
Sends the electronic cash to the TTP but wants to withdraw	Sends the digital product to the TTP and wants to continue the transaction	Protocol terminates
Sends the electronic cash to the TTP but wants to withdraw	Sends the digital product to the TTP but wants to withdraw	Protocol terminates

3.0 PROTOCOL COMPARISONS

Protocols that provide both anonymity and fair exchange are taken and every protocol's disadvantage(s) have been stated and is compared against the proposed protocol to see whether or not the proposed protocol overcomes the mentioned disadvantage(s).

3.1 IMPOSING FAIRNESS VS. FRANKLIN & REITER'S FAIR EXCHANGE PROTOCOL

The disadvantages of Franklin & Reiter's Protocol and how Imposing fairness Protocol overcomes the same are listed in the table below.

Franklin & Reiter	Fahad
Semi-Trusted TTP	Fully trusted third party
Assumes only one party is dishonest at any given point in time and hence does not provide a solution when two parties are dishonest.	Assumes that any party can misbehave and has a feature whereby the protocol terminates in any case where dishonesty is detected
Provides only partial anonymity	Provides full anonymity

3.2 IMPOSING FAIRNESS VS. RAY'S ANONYMOUS & FAILURE RESILIENT PROTOCOL

The disadvantages of Ray's protocol are listed in the below table and how Imposing Fairness protocol is designed to overcome the disadvantages mentioned are shown.

Ray	Fahad
It uses pseudo-identifiers to provide anonymity. A customer is required to generate these pseudo-identifiers and when customers generate a new one for every transaction, this results in a bottle neck.	Anonymity is provided by means of using electronic cash and also secure channels. This does not create any overhead.
Verification of the protocol by Kong et al [14] clearly shows that the Trusted Third Party is not entirely trustworthy	The Third Party here is entirely trustworthy as the protocol assumes that none of the parties can be trusted and takes steps to overcome this problem.

3.3 IMPOSING FAIRNESS VS. ANONYMITY AND FAIR EXCHANGE BY ZHANG

The table below lists the disadvantages of Zhang's Anonymity and Fair Exchange Protocol and compares it against Fahad's Imposing Fairness Protocol.

Zhang	Fahad
Too many messages	Only 7 messages across all phases
It does not assure fair exchange through all the phases of the transactions. It does not cover the withdrawal phase	Fair exchange is guaranteed throughout all the phases of the electronic commerce transaction
Customers are required to disclose the public key during the transactions. Using the same key again and again might allow the merchants to trace the customer thus compromising on the anonymity feature.	Since electronic cash is being used, this is virtually untraceable and hence provides complete anonymity

3.4 IMPOSING FAIRNESS VS. ZHANG'S MUTUAL AUTHENTICATION PROTOCOL

The table below clearly indicates the shortcomings of Zhang's Mutual Authentication Protocol and shows how these shortcomings are tackled by the proposed Imposing Fairness Protocol

Zhang's Mutual Authentication Protocol	Fahad
Too many messages – 6 phases and 11 messages	Only 7 messages in total
It is very cumbersome as it has a lot of phases	The proposed protocol does not have iterative phases and hence very efficient and fast
It has a commit buffer that is being used by the Trusted Third Party and assumes that the commit buffer is always sufficient and available. If the commit buffer is not available the protocol fails and it does not provide any solution when this happens.	It does not make use of any buffers and the protocol has thoroughly been analysed to ensure it is available.

3.5 SUMMARY

From the comparisons based on different criteria, it can be clearly understood that the proposed protocol fares a lot better than all the other protocols and also effectively and efficiently overcomes the disadvantages of the other protocols which indicates the novelty of the protocol.

4.0 MODEL CHECKING & EVALUATION

This section describes the model checking tool that was used and also describes in detail the outcome of this formal verification process. It aims to describe areas that require attention and helps prove that the protocol has been thoroughly analysed and that the protocol satisfies all its pre-determined key properties thus fulfilling the research aims.

The tool that has been used for the formal verification of the proposed protocol is called as the Moonwalker. Moonwalker is a software model checker tool that is used for Common Intermediate Language (CIL) bytecode programs. CIL programs are those programs that are written for the .NET platform. The MoonWalker tool is based on Mono C# Compiler that is used to run the C# compiled bytecode (.NET).

The MoonWalker software tool uses an approach called as the Virtual Machine (VM) approach for the purposes of model checking and verification. This means that every byte of the CIL code that is fed is thoroughly analysed and every state of the code is systematically studied and verified.

Unlike many other software tools for model checking, MoonWalker does allow code from different languages to be run and verified. It was earlier known as the Mono Model Checker but was renamed to MoonWalker due to the name clashes. The design is inspired by the Java Path Finder, a model checker for Java programs.

The later versions of MoonWalker have many improvements added. These enhancements were added in order to improve the usability of the tool and to augment the user-experience. In simple terms, the later version is more user friendly and has a more effective error-tracker that does not confuse the user. Extensive test framework to detect most flaws in logic and flows are also added to the recent version.

From Model checking, it has been clear that there has been no assertion violations or deadlocks in the protocol's prototype.

The following table shows the execution time statistics for every individual program code of the protocol. This was analysed by the model checker as follows:

Program	Time
Execution time for Compile.exe	0.03 seconds
Execution time for Certificate.exe	0 .109 seconds
Execution time for EncryptedProduct.exe	0.09 seconds
Execution time for Order.exe	0.109 seconds
Execution time for Payment.exe	0.09 seconds
Execution time for Product.exe	0.09 seconds
Execution time for Verification.exe	0.109 seconds

The below table shows the statistics for the total memory used by every individual program's executable file run. Effective usage of memory determines how efficient the code is and also ensures that there is no garbage.

Program	Memory used for the executable file run
Current memory for Compile.exe	33672 KB
Current memory for Certificate.exe	32636 KB
Current memory for EncryptedProduct.exe	33048 KB
Current memory for Order.exe	33040 KB
Current memory for Payment.exe	33216 KB
Current memory for Product.exe	32664 KB
Current memory for Verification.exe	32640 KB

The above table shows that the memory space that each program takes up individually is not very huge and the evaluation of this aspect shows the efficiency of the protocol.

5.0 CONCLUSION

The following criteria have been used to determine the success of the research.
, the following criteria are described.

1. Development of the protocol
   There are a number of fair exchange, optimistic protocols that are available. The research aims at analysing the existing protocols, identify the gaps and propose a protocol that is efficient and that overcomes the issues identified. The protocol would then be compared against the criteria mentioned and checked how much it helps overcome issues and gaps identified.
2. Automated Dispute Resolution
   In some cases or instances disputes are bound to arise between the transacting parties namely the merchant and the customer. The aim of the protocol is to minimise issues and also providing automated dispute resolution in situations that are inevitable.
3. Fairness and anonymity
   The aim of the protocol is to provide fairness by ensuring that either both or none of the transacting parties gets the items and also providing anonymity for the customer's private information. The protocol aims at providing optimistic fair exchange.
4. Protocol Analysis:
   The protocol that has been proposed is analysed completely in all given circumstances and scenarios and formally verified. Furthermore, all dispute scenarios are clearly identified.
5. Model Checking and verification

From this, it can be understood that the research addresses the gaps in the current literature and also contributes significantly. The protocol proposed is novel and addresses all the issues and provides an effective and efficient protocol.

REFERENCES

[1] F. Bao, R.H. Deng and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP", Proceedings of the IEEE Symposium on Security and Privacy, pp. 77-85, Oakland, California, USA, 1998.

[2] I. Khill, J. Kim, I. Han and J. Ryou, "Multi-party fair exchange protocol using ring architecture model", Computers & Security, Vol. 20, No. 5, pp. 422-439, 2001.

[3] I. Ray, I. Ray and Z. Narasimhamurthi, "An optimistic fair-exchange electronic commerce protocol with automated dispute resolution", Lecture Notes in Computer Science, Vol. 1875, pp. 84-93, 2000.

[4] I. Ray, I. Ray and N. Natarajan, "An anonymous and failure resilient fair-exchange electronic commerce protocol", Decision Support Systems, Vol. 39, No. 3, pp. 267-292, 2005.

[5] Q. Zhang, K. Markantonakis and K. Mayes, "A practical fair-exchange e-payment protocol for anonymous purchase and physical delivery", Proceedings of the 4th IEEE International Conference on Computer Systems and Applications, pp. 851-858, Dubai, UAE, 2006.

[6] Q. Zhang, K. Markantonakis and K. Mayes, "A mutual authentication enabled fair-exchange and anonymous e-payment protocol", Proceedings of the 8th IEEE Conference on Electronic commerce Technology and the 3rd IEEE Conference on Enterprise Computing, Electronic commerce and E-Services, pp. 20-27, San Francisco, California, USA, 2006.

[7] N. Zhang, Q. Shi and M. Merabti, "A unified approach to a fair document exchange system", The Journal of Systems and Software, Vol. 72, No. 1, pp. 83-96, 2004.

[8] N. Zhang, Q. Shi, M. Merabti and R. Askwith, "Practical and efficient fair document exchange over networks", Journal of Network and Computer Applications, Vol. 29, No. 1, pp. 46-61, 2006.

[9] Zhang et al, "A Practical Fair Exchange E-payment protocol for anonymous purchase and physical delivery", IEEE conference on System & Application, 2006

[10] Zhang et al, "An Efficient Protocol for Anonymous and Fair Exchange", Computer Networks, 2003