Achieving Fair Exchange and Customer Anonymity for Online Products in Electronic Commerce

PhD Thesis

FAHAD ALI ALQAHTANI

This thesis is submitted in partial fulfilment of the requirements for the decree of Doctor of Philosophy

Software Technology Research Laboratory

De Montfort University

Leicester - United Kingdom

June 2014

Declaration

I declare that the work described in this thesis is original work undertaken by me for the degree of Doctor of Philosophy at the Software Technology Research Laboratory (STRL) at De Montfort University, United Kingdom.

No part of the material described in this thesis has been submitted for award of any other degree or qualification in this or any other university or college advanced degree.

I also declare that part of thesis has been published in some of the following publications

JOURNAL PUBLICATION:

1. Fahad A. AlQAHTANI: Imposing fairness in electronic commerce Using Trusted Third Party for electronic product delivery. International journal of computer science issues,Vol.11,issues 1,No 2,January 2014

2. Fahad A Alqahtani : A Fair Exchange and Customer Anonymity Protocol Using A Trusted Third Party for E-Commerce Transactions and Payments. International Journal of Network Security and Its Applications (IJNSA), Vol.6, No.1, January 2014

Acknowledgements

In the name of Allah, the Most Gracious and the Most Merciful.

First and foremost, all praise is due to Allah for giving me the strength, energy, and patience to complete this thesis. It is now complete because of the support of many people to whom I owe my deepest gratitude.

It gives me great pleasure to acknowledge the support and help of my first supervisor Dr. Ali Al-Bayatti. His wisdom, knowledge and commitment have inspired and motivated me during these years. Special thanks also go to my second supervisor Antonio Cau, many thanks for the STRL staff.

I wish to express my love and gratitude to my beloved families; my father Ali, mother Nora, brothers and sisters for their understanding and endless love through the duration of my studies.

I am much indebted to my wife, without whom this work would have never existed. For her love, support and patience since we came to UK. For looking after our children; Arwa, Ali, Zyad, and Thamer.

Finally, I offer my regards and blessings to all of those who supported me in any respect during the completion of the thesis.

Abstract

In the recent years, e-commerce has gained much importance. Traditional commerce (in which case the customer physically goes to the merchant's shop, purchases goods and/or services and makes a payment) is slowly being replaced with e-commerce and more people tend to prefer doing their shopping online. One of the main reasons for this attraction is the convenience the e-commerce provides. Customers can choose from a lot of different merchants at the convenience of their homes or while travelling by avoiding the hassle and stress of traditional shopping. However, e-commerce has lots of challenges. One key challenge is trust as transactions take place across territories and there are various legal & regulatory issues that govern these transactions.

Various protocols and underlying e-commerce technologies help in the provision of this trust. One way to establish trust is to ensure fair exchange. There is also a question about traceability of transactions and customers' need for privacy. This is provided by anonymity – making sure that the transactions are untraceable and that the customers' personal information is kept secret. Thus the aim of this research is to propose a protocol that provides fair exchange and anonymity to the transacting parties by making use of a Trusted Third Party. The research is also aimed at ensuring payment security and making use of a single payment token to enhance the efficiency of the protocol.

The proposed protocol consists of pre-negotiation, negotiation, withdrawal, purchase and arbitration phases. The analysis of the protocol proves that throughout all the phases of the e-commerce transaction, it is able to provide fair exchange and complete anonymity to the transacting parties. Anonymity provides the privacy of customers' data and ensures that all Personally Identifiable Information of the transacting parties are kept hidden to avoid misuse. The protocol proposed is model checked to ensure that it is able to show that the fair exchange feature is satisfied. It is implemented using Java to show that it is ready-to-use and not just a theoretical idea but something that can be used in the real-world scenario. The security features of the protocol is taken care of by making sure that appropriate cryptographic algorithms and protocols are used to ensure provision of confidentiality and integrity.

This research explores those areas that have not been covered by other researchers with the idea that there is still a lot of scope for improvement in the current research. It identifies these

opportunities and the 'research gaps' and focuses on overcoming these gaps. The current e-commerce protocols do not cover all the desirable characteristics and it is important to address these characteristics as they are vital for the growth of e-commerce technologies. The novelty of the protocol lies in the fact that it provides anonymity as well as fair exchange using a Trusted Third Party that is entirely trustworthy unlike certain protocols where the trusted third party is semi-trusted. The proposed protocol makes use of symmetric key cryptography wherever possible to ensure that it is efficient and light weight. The number of messages is significantly reduced. This overcomes the drawback identified in various other protocols which are cumbersome due to the number of messages. Anonymity is based on blind signature method of Chaum. It has been identified that usage of other methods such as pseudo-identifiers have resulted in the inefficiency of the protocol due to the bottlenecks created by these identifiers. It also ensures anonymity can never be compromised unlike certain protocols whereby an eavesdropper can find out the customer's identity as the customer is required to disclose his/her public key during transactions. Further to this, the protocol also provides immunity against message replay attacks. Finally, the protocol always assumes that one or more parties can always be dishonest which is unlike certain protocols that assume only one party can be dishonest at any point. This ensures that all scenarios are taken into consideration and two parties cannot conspire against the other thus compromising on the fairness of the protocol.

Detailed analysis, implementation, verification and evaluation of the protocol is done to ensure that the research is able to prove that the protocol has been carefully designed and the key goals of fair exchange and anonymity. All scenarios are taken into consideration to prove that the protocol will indeed satisfy all criteria. The research thus expects that the protocol could be implemented in real-life scenarios and finds a great potential in the e-commerce field.

List of Tables

List of figures

Glossary

TTP	Trusted Third Party. An entity that is believed to be unbiased in a transaction between the Merchant and Customer
CA	Certificate Authority. An entity that can produce certificate by verifying the signature of the claimed entity.
NIST	National Institute of Standards and Technology. An institute that aims at standardising technology
ICO	Information Commissioner's Office. All data breaches in the UK needs to be reported to the ICO
Producer	The creator of the digital product who owns the copyrights for the product
Encryption	Process of changing plaintext into cipher text using an algorithm and a key
Decryption	Process of changing cipher text to plain text using an algorithm and key
Key	A secret that is used to encrypt or decrypt (similar to a passwords)
Hash	A one way function that takes variable length input and provides a fixed length output making it mathematically impossible to determine the plaintext from the cipher text
Fair Exchange	A transaction where neither of the transacting parties get undue advantage
Anonymity	A condition in which an individual's identity is kept secret

Privacy	The data relating to individuals kept secret
Confidentiality	An information security goal whereby the data is not accessible to any unauthorised users
Integrity	An information security goal whereby data cannot be modified by unauthorised users either accidentally or intentionally
Availability	An information security goal whereby data is available at the right time to the right user
Non-Repudiation	An information security goal whereby a user or an entity cannot deny having sent or received information or performing tasks
Arbitration	A process by which a neutral party collects information from parties in dispute and makes a decision based on the evidence
Mediation	A process similar to arbitration but the mediator does not make decision
Payment Gateway	Set of servers usually connecting to the private network of the bank or financial institutions in a secure manner

Table of Contents

CHAPTER 1: INTRODUCTION

The aim of this chapter is to provide a broad overview of both e-commerce and the intended research. It offers a platform that would enable the reader understand the need for this research and also provides a gist about recent developments both in the industry and in research circles with respect to electronic commerce.

Chapter Objectives:

- Describe to the reader the e-commerce terminology, growth, advantages and disadvantages as well as recent developments in this area
- Understand the background, motivation and research process
- Describe the central research question and discuss in detail the contributions of this research
- Explain how the thesis is organised
- Describe the success criteria for the research

1. 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 not only to be able to connect with anybody, anywhere anytime but also to make purchases at a click of the mouse and at their most convenient time. Furthermore, consumers' reliance on technology has also increased dramatically, which now makes electronic commerce (e-commerce) one of the most promising markets for merchants. Given that these technologies are developing at a very rapid pace, it is evident that internet markets and the potential for e-commerce will continue to flourish for the next few decades.

E-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. Not only have there been changes in the technological arena, but changes have also been engendered in the business models and in the way businesses operate. For example, the manner in which businesses now reach customers has drastically changed. Various business models are now being adopted, such as subscription to online services whereby the customer pays a fixed sum at specific times to enable them access and benefit from a specific service. Another such business model is pay-per-use; this is commonly used in e-commerce transactions involving digital services for the purposes of downloading music, video or software. This does not bind the customer to a specific provider (as the subscription model does), rather, it affords the customers the flexibility to choose from a variety of service providers and to pay only for what they use (Y Zhang, 2013).

E-commerce is gaining in popularity these days, for many reasons; however, the most popular ones are the following (Y Zhang, 2013):

1. E-commerce obviates the need for the customer to physically travel to the merchant in order to purchase goods or services. It enables the customer to purchase the same goods online with ease and also at a time that is suitable to them without having to worry about opening and closing hours (unlike in traditional commerce).
2. Given that all the relevant information is available to the customer on the internet website, and given the fact that there are many merchants trying and sell similar

products, customers are able to compare prices, have plenty of options, read reviews from other customers and buy those products that suit their budget.

3. Customers can purchase from anywhere in the world depending on the willingness of the merchant to deliver. This accords customers additional choices and they are not restricted by geographical and territorial boundaries.

(Y Zhang, 2013)

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. The customer cannot be sure that he/she will receive the goods that he/she has ordered, and hence there is an issue of trust involved here. From the point of view of the merchant, a transaction represents a risk; this is because he/she is obliged to send the product to an entirely unknown entity. Similarly, from the point of view of the merchant, he/she will not be sure that the funds received would be materialised until the money is deposited in the bank account.

It also poses many questions for the customer, such as: How can I trust that the goods that I have ordered will definitely reach me? Or what happens if I cancel the transaction; will I be wrongly charged? Or how will my online identity be protected, and how secure are the personal details that I gave when registering with the website? The customer may be concerned about the protection of online identity so that in the future he/she is not bombarded with spam or subjected to identity theft. As most payments are traceable, customer may also be worried about the merchant tracking their purchasing habits, thus raising privacy issues. In the traditional commerce environment, this problem is resolved as the customer has the option of paying for the goods and/or services in cash. This eliminates any concern that the customer's financial information may be disclosed. In an e-commerce scenario, there is also the issue of the theft of any financial data that is stored and/or transmitted electronically. To avoid any misuse of this information, adequate measures need to be taken to ensure that the data are encrypted whilst being stored or transmitted over the internet to the merchant.

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

of the customer remains concealed (data anonymity) in order to ensure privacy for the customer. This protocol is different from Paypal and other similar service providers as it does not retain a part of the service charge as commission and is strictly tied on to the e-commerce transaction in process and not designed as a payment mechanism like Paypal.

Certainly, the internet eases the buying and selling of goods and/or services across the globe. However there are key issues relating to security, trust and anonymity. It is essential that the technologies and the protocols used to facilitate e-commerce transactions are able to ensure that these aspects are well taken care of while also making sure that process is simple and not unnecessarily complicated. Thus, the main idea of the research is to propose an e-commerce protocol that will ensure that both of 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 undisclosed.

1.1 Background

Boston Consulting Group recently conducted a study on e-commerce trends and found that the UK is one of the most internet-aware markets in the world, with internet sales representing 8.3% of the economy, with a total worth of £121 billion, which accounts for almost 13.5% of total sales. The study also indicates that this will rise to 23% by 2016. Nearly 32 million people in Great Britain (which accounts for 66% of all adults) have used e-commerce technologies to buy products and services online (New Media Trend Watch, 2013).

In the traditional marketplace, there is a certain level of trust between the vendor and the customer, as they can see each other and in some cases have already established a relationships and some measure of goodwill. However, in case of an e-marketplace, trust is a key concern because transactions may take place across great distances and even across national borders; there are various legal and regulatory issues that govern such transactions. Trust in e-commerce is an issue for a number of reasons.For example, lack of brand recognition could make it difficult for customers to really know the brand. Many retailers have only an electronic presence and hence customers may not be aware of the new brand. Secondly, natural distrust in e-payments; customers have a natural distrust when it comes to making online payments. This issue arises because customers are not sure how their data are stored or viewed. Thirdly, there is a limited understanding over the legal issues relating to e-commerce, shortage of persons trained in

understanding the legal complexities or who can give advice to aggrieved customers and differences amongst countries in terms of legislation, capacity to import/export goods, resources available, et cetera. Research also shows privacy and data protection also concerns users as not every country has sufficient regulation (Maity and Dass, 2014).

Grau (2006), in his research report, discusses the importance of privacy. Privacy refers to avoiding the misuse of any personal data collected or to preventing the collection of excessive or unnecessary data from the user. Grau also discusses how people are generally reluctant to use online payment systems due to perceived security issues and concerns relating to privacy, i.e. to Personally Identifiable Information (PII). Provision of Anonymity is a means toward achieving customer privacy; this also helps to increase trust from the viewpoint of the customer. A customer is more likely to visit a website that provides anonymity or where the customer believes that his/her personal data will not be misused. It is thus imperative that e-commerce websites state how personal data are stored or used; this promotes customer confidence and thus increases trust.

1.2 Motivation

As discussed above, Anonymity and Fair Exchange plays a pivotal role in the provision of trust. There are many protocols in the literature that concentrate on Fair Exchange (Bao, 2998; Khill, 2001;Ray, 2000; Ray, 2005; Zhang, 2003; Zhang et al, 2006;Zhang, 2004; Zhang & Shi, 2006). However, only a very few of these protocols concentrate on both anonymity and fair exchange aspects (Ray, 2005; Zhang, 2006; Zhang, 2003). Though these three protocols address fair exchange and anonymity, there are various weaknesses, some of which are inherent. One for example relates to the number of messages sent between the transacting parties and also to the fact that the Trusted Third Party (TTP) is not entirely trustworthy; the TTP is capable of viewing and/or modifying a message. Although these protocols ensure that the TTP does not collude with a particular party, they do not guarantee that the TTP is genuine and impartial. Also, they do not provide any mechanism for tackle a situation where the TTP modifies the message sent by either the customer or the merchant, thus becoming semi-trusted.

Normally, a TTP is an unbiased party or an arbitrator that facilitates smooth transactions between two or more parties. In reality, however, there are opportunities for the TTP to exploit transactions for personal benefit. Where there is the chance of such an event occurring, the TTP

is categorised as a semi-trusted party, as opposed to the ideal scenario of the TTP being entirely trustworthy.

Various protocols used in e-commerce provide certain security features, assisting in the establishment of trust by providing mechanisms for Fair Exchange, Anonymity, Dispute Resolution and Non-Repudiation (of the transaction). Though there are various desirable characteristics that an e-commerce protocol should possess, Zhou and Gollman (1996) formalised these characteristics and defined the conditions that any e-commerce protocols should satisfy. There are five key such characteristics defined in their paper. The main characteristics include fair exchange, dispute resolution, assurance,trusted third party and commitment to the transaction.

All the features mentioned above are not implemented by all protocols. However, most of the e-commerce protocols provide most or all of the features mentioned above. In short, the above characteristics are very much desired; however, due to practical limitations, only a subset of these features is incorporated by the protocols.

One of the other motivations for conducting this research is to address another key challenge in e-commerce protocols: providing anonymity along with fair exchange. Designing a protocol with a mechanism to safeguard the customer's details thus represents a key question on which to focus. This is essential as it assists in providing privacy for any data relating to the customer, and also ensures that the merchant cannot track the customer or misuse those data for any other purpose.

The following chapters discuss in detail the various technical drawbacks of these protocols and also the motivation for researching a new protocol that would help eliminate the discussed technical drawbacks.

The research will mainly focus on designing a protocol that would ensure fair exchange and anonymity. It will make use of a Trusted Third Party (TTP) also ensure that the TTP is unable to masquerade or take undue advantage of the situation. This means that the TTP is forced to be honest and thus does not have the authority to view or modify the messages sent. Since in most cases the Trusted Third Party is partially trusted and it is not very realistic to be able to ensure

that TTP is entirely trustworthy, this protocol enforces certain means to make sure the trust between the parties is not breached.

1.3 Objective & Central Question

Given the background and the motivation of this research, the purpose of undertaking this research or the key objectives of this research are described in this section of the document. There are various protocols that provide fair exchange and discuss the problems of e-commerce trust using various methods. However each protocol has various disadvantages.

The key objective of this thesis is to compare the key protocols that provide fair exchange, anonymity and built in dispute resolution to identify the technical flaws, drawbacks, limitations and gaps. Once this is done, the gaps are identified and areas that needs to be improved or enhanced. This also helps to justify the need for the new protocol and the need to place controls on the Trusted Third Party to ensure that there is no breach of trust due to the partially trusted nature of TTP. Given that fair exchange and anonymity are key components of a trust-based e-commerce protocol the thesis aims at developing a protocol that would overcome the flaws that are identified and in addition keeping in mind that confidentiality and integrity of the messages exchanged between the merchant and the customer are maintained.

The key research problem that is identified is derived from the current research; it could be the case that there are too few effective and efficient e-commerce protocols that provide the characteristics below:

- Fair exchange through all the phases of the e-commerce transaction
- Total customer anonymity
- The Trusted Third Party by nature is partially trusted. The TTP should however be restricted from reading or modifying messages and masquerading.
- Built-in dispute resolution mechanism
- Termination of the protocol when either party behaves dishonestly
- Efficient and effective purchase mechanism (not cumbersome and with a limited number of messages)

Therefore, the central research question is as follows:

Is it possible to design an e-commerce protocol that uses a TTP by ensuring that its partially trusted nature is circumvented to provide fair exchange throughout all phases of the transaction in addition to providing anonymity for the customer and a built-in dispute resolution?

1.4 Contribution

The research develops a robust protocol that would provide both anonymity and fairness. The key contribution of this research is combining these two properties in a protocol and achieving effective dispute resolution mechanism based on a Trusted Third Party and also with minimal messages. The novelty lies in the fact that this protocol provides not just anonymity of customer data but also fairness all throughout the e-commerce phases.

The first contribution is the protocol that provides the following features:

- A simplified protocol that helps in the provision of fair exchange to enforce honesty between the transacting parties.
- It helps in the development of a new protocol that would provide anonymity and fair exchange.
- Circumventing the partially trusted nature of TTP by placing controls
- Avoid Replay attacks
- Provide payment security
- An inbuilt dispute resolution mechanism

The second contribution is the implementation and model checking

- The implementation of the proposed protocol to ensure that it is ready for adaptation in the real-world
- Model checked to ensure that the protocol is viable and the logic is correct.

1.5 Measuring Success

At the end of the research, to determine the research success, it is necessary to ascertain that certain key points are achieved. These points or success criteria enable measuring the level of achievement of the research and assist in determining whether the research has made a significant contribution. These key points are to be used as guidelines for establishing how successful the research has been in terms of achieving the key objectives discussed. In order to measure the success of the research, the following criteria are described.

- The first measure of success is to evaluate the protocol to check if the research questions are answered. Answering the research questions appropriately .
- An in depth analysis to determine the difference between various other protocols and the proposed protocol to show how efficient it is.
- Development of the protocol: There are a number of fair exchange protocols available. The research aims at analysing the existing protocols, identifying the gaps and proposing a protocol that is efficient and that overcomes the issues identified. The protocol would then be compared against the criteria mentioned and checked how far it helps overcome the issues and gaps identified.
- Specifying the effectiveness criteria of the protocol: the proposed protocol would clearly indicate how many messages are sent and the contents of messages.
- 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 to provide an automated dispute resolution mechanism in situations where there are disputes.
- Protocol analysis: The proposed protocol is analysed completely in all given circumstances and scenarios, and is formally verified. Furthermore, all dispute scenarios are clearly identified.
- Having a good proof of concept by implementing the protocol to prove that it could be adopted in real-world scenarios and also to check for the output data flows and to identify issues, bugs and errors.

- Model checking and verification: The proposed and implemented protocol is model-checked and verified thoroughly to validate the logical flow of steps, and also to determine that the protocol successfully satisfies all the key criteria mentioned. In simple terms, this assists in establishing that the protocol implements fair exchange, anonymity and payment security throughout all stages. It also helps identify any deadlock situations that might prevent the protocol from running successfully.

In summary, this chapter has provided a brief overview of the research, addressed the key challenges or gaps in the literature and justified the need to conduct this research. This chapter has also set the background and motivations for the research in order to enable the reader to better understand the subsequent chapters. The central question for the research has addressed here, and the reader now also understands the problem statements that have led to this research.

1.6 Thesis Structure

The thesis structure is as follows. Chapter 1 provides the introduction to the research, a brief about the key research questions, the objectives of the research and the research contribution. It also gives a list of factors that would contribute to the success of the research.

The second chapter discusses the research methodology and also the research process that has been adopted by the research.

The third chapter provides the literature review and discusses topics relating to e-commerce, trusted third party, legal and regulatory aspects of e-commerce , fair exchange, data privacy , anonymity and also various protocols providing these.

The fourth chapter provides an overview of various cryptographic concepts used in the protocol along with the assumptions made.

The fifth chapter provides a detailed description of the proposed protocols and also provides an analysis.

The sixth chapter compares the protocols using various Key Performance Indicators as well as with other protocols.

Chapter 7 discusses the protocol's implementation and the key concepts and components of the implementation.

Chapter 8 shows the verification of the protocol, Model Checking, the process and analysis. The final chapter provides a summary of the research, revisits the success criteria and discusses the protocol's contribution. The limitations and future work is also discussed in this section.

1.7 Summary

The introduction has enabled the reader to understand the key challenges in the e-commerce arena, and how these can be addressed. This chapter has also given the reader an in-depth understanding of how these concepts interrelate and how they are implemented or adapted in the real world; this is to enable the reader understand the role that trust plays in the e-commerce environment.

The reader has been introduced to the concepts of trust, fair exchange and anonymity although the following chapter will give more detailed descriptions and insights derived from the literature review. The chapter has concluded by specifying the key success criteria that are to be used at the end of the research in order to determine how successful it has been and also to demonstrate the contributions that the research has made.

CHAPTER 2: RESEARCH METHODOLOGY

The aim of this chapter is to provide a brief of the research methodology used for the research and discuss the research process.

Chapter Objectives:

- Introduce the reader to the research methodology
- Discuss the research process

2.1 Research Process

The success of the research is admittedly determined by measuring the extent to which each of the research objectives is met. The following steps are followed during this research to ensure its success. These steps are as follows:

Firstly, a background into the research and its motivations is given. Following this, the key literature in this area is thoroughly investigated. This is intended to ensure that all aspects of the research are identified and that the technical challenges or gaps in the current literature are identified and clearly understood.

Once the gaps in the current literature are understood, the key research objectives are drafted and the research contribution is carefully analysed. It also discusses the key characteristics that e-commerce protocols should ideally possess.

It then aims to design the protocol as mentioned in the objectives and it finally lists future work and areas for improvement.

In short, the research process is summarised in the flow chart below (Fig. 1).

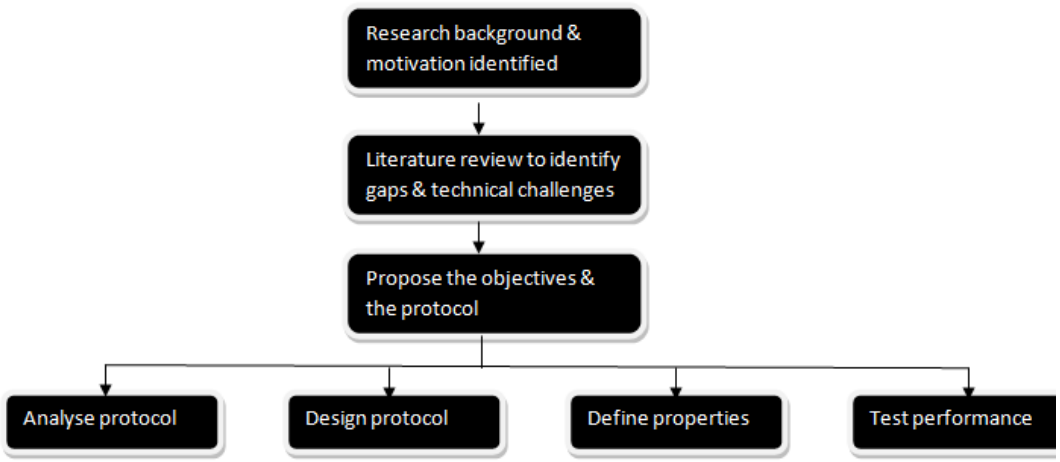


Figure 2.1: The research process

2.2 Research Methodology

The methodology employed in this research is described in detail in this section. The above diagram demonstrates the various processes involved in the thesis; for any research to be successful, adequate steps need to be taken in order to ensure that the method for conducting it is well thought out and that all areas of the research process are addressed. This enables the researcher not only to understand the key challenges but also to meet those challenges with preparedness and ease. A constructive research methodology is adopted in this research. In a constructive research methodology,a new contribution to the research is referred to as the construct. This involves clearly identifying objectives, identifying a process for finding out the research gaps, prepare simulation, run simulation and give feedback on the results (Crnkovic, 2010) The following methodology has been adopted for the purposes of this research.

- Gathering data and comprehending the field:

  The first step in this process entails a detailed research into the existing literature. All relevant literature must be collated in order to understand the gaps and also to gain a deep understanding of the underlying technologies. The aim of this task is also to help formulate a roadmap for the protocol process and also to correctly establish the line of research. This enables identification of the central question of the research and helps to understand why other researchers have used certain specific methods to achieve their research goals.

  Various books and online referencing exploiting search engines such as Google are utilised. Research papers from IEEE, ACM and SpringerLink are also being used.

- Analysis:

  This step assists in identifying all the key protocols; it entails analysing each and every e-commerce protocol in order to understand their core strengths and weaknesses. It also helps to gain a better understanding of the various cryptographic techniques used to achieve the desirable qualities of the protocols, and to comprehend why these techniques were being used in the first place.

- Theoretical design:

  Analysis of the protocols helps to identify gaps and this step will further assist in the literature review and in framing the central research question. The theoretical design

stage then assists in formulating the actual protocol and in describing how this protocol overcomes the weaknesses identified in the other protocols; it also reveals the key areas it shall contribute.

- Implementation:

  The theoretical design stage now has the protocol and steps in detail. The next stage of the research is to implement the proposed protocol to demonstrate a workable prototype. This is done in order to show that the protocol is feasible in the real world, and also to informally test and verify any flaws within the protocol.

- Evaluation, model checking and verification:

  This is the final stage in the research process, whereby the protocol is formally evaluated and verified. Model checking is conducted to ensure that the protocol's design flaws are identified, statistics are obtained and any errors that might have been missed in the previous steps are captured. It also helps to identify deadlocks, flaws in the logic or design of the protocol, and the steps whereby further developments can take place.

The flowchart Figure 2.2 below gives a clear picture of the research methodology. Please note that this is an iterative process and will continue until the research is completed (taking into account the thoroughness of the literature review) and until all the research goals are satisfied.

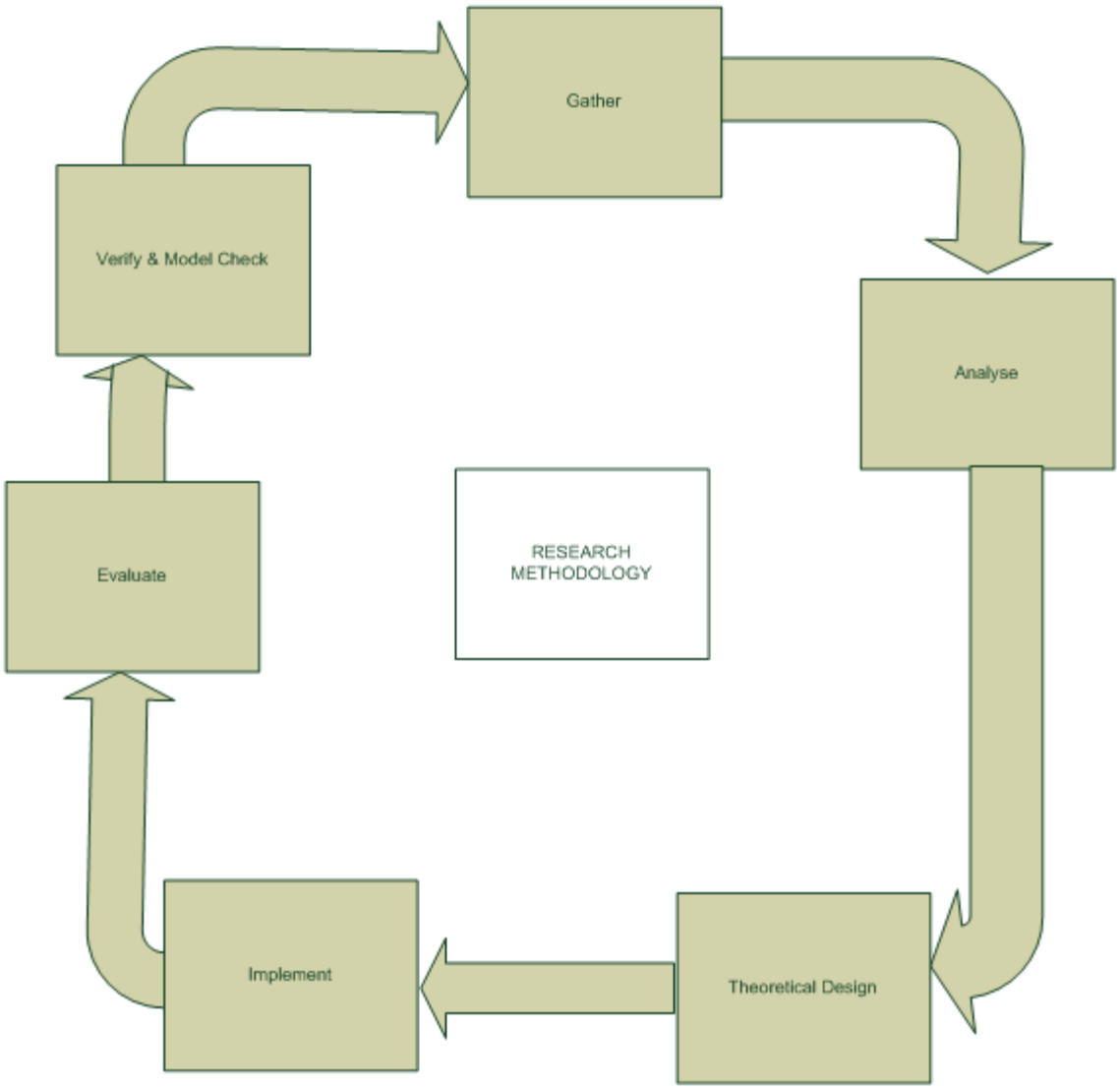


Figure 2.2: The Research Methodology

2.3 Summary

In this chapter, the research process has been clearly defined and this should assist the reader in understanding how the research is to be conducted and how it is to produce the desired results. The reason for selecting the research methodology and the steps involved in answering the research question has been discussed in this chapter.

CHAPTER 3: LITERATURE REVIEW

The aim of this chapter is to give a broad overview of the various key literatures that are being utilised in this research. It includes all the main topics such as e-commerce, security, digital payment, anonymity, fair exchange, et cetera.

Chapter Objectives:

- Introduce the reader to the various literatures and key terminologies that are to be used throughout the research.
- Understand the various protocols that are being used as well their shortcomings, and identify any gaps in current research.
- Explain various e-commerce protocols in detail along with the steps that are being used in each and every protocol; diagrams of each protocol and the mechanisms and techniques these protocols use shall be explained.

3 Literature Review

The main aim of this chapter is to discuss in detail all the related literature. It is imperative to read and review the existing literature as the purpose of this research is to propose a new and efficient protocol that would overcome the negatives or the drawbacks of the existing ones. This new protocol aims at providing privacy/anonymity and true fair exchange in such a manner that ensures that the Trusted Third Party (TTP) which is by nature partially trusted is circumvented by not allowing to modify the messages and that the exchange of the digital products is both effective and efficient. The literature review first discusses what e-commerce actually means and then walks through various other terminologies and concepts. The literature also aims to introduce the basic cryptographic mechanisms and concepts that would be used in the protocol that is to be proposed. Furthermore, it also covers other aspects that are indirectly related to this research, and these include electronic cash, verification techniques, and model checking methodologies and tools. The literature is broken down into the main areas and starts by discussing the two key attributes, namely fair exchange and anonymity, and describes in detail the current key research in those areas.

3.1 E-commerce

This research addresses e-commerce protocols that facilitate the smooth processing of transactions and the purchasing of goods and services between two parties, namely the customer and the merchant, over the internet; but what exactly is e-commerce? The business dictionary defines electronic commerce or e-commerce as, "*Business conducted through the use of computers, telephones, fax machines, barcode readers, credit cards, automated teller machines (ATM) or other electronic appliances (whether or not using the internet) without the exchange of paper-based documents. It includes activities such as procurement, order entry, transaction processing, payment, authentication and non-repudiation, inventory control, order fulfilment, and customer support. When a buyer pays with a bank card swiped through a magnetic-stripe-reader, he or she is participating in e-commerce.*" (Business Dictionary, 2013)

There are various other definitions as well. Roger Clarke (2000) defines e-commerce as follows: "*the conduct of commerce in goods and services, with the assistance of telecommunications*

and telecommunications-based tools; some people use the term 'electronic trading' to mean much the same thing. Others use 'electronic procurement', 'electronic purchasing' or 'electronic marketing'."

He discusses the different segments that constitute e-commerce, which include the following terms and concepts: (Clarke, 2000)

Electronic catalogues: a means whereby sellers or merchants can communicate effectively with buyers (or potential buyers) about the services they provide or the products they offer.

Electronic Data Exchange (EDI): standards (or the family of standards) that are used for expressing the structured data during e-commerce transactions.

The author further provides details about the various phases that are involved in an e-commerce transaction; he details six key stages or phases in every transaction. This model or phased approach comes in very handy and is extremely useful when analysing the application of specific technologies or protocols to e-commerce. The author explains that the six phases listed are easily identifiable in most real-world scenarios as they are quite distinct. However, in certain cases, one or two phases could be merged or there might be a change in the order or sequence of the phases (or they could overlap each other). (Clarke, 2000)

The phases described by the author include the following:

(1) The Pre-Contractual Phase

This is the first phase in any e-commerce transaction. At the commencement of the process, the buyer and merchant are concerned with the collection and gathering of market data and intelligence. The buyer is concerned with information on the various suppliers of the required goods or services, the goods or services themselves, the prices, availability, the terms and conditions applicable to a purchase, logistics, and the legality of buying a specific product and/or service. The buyer is also concerned with the authenticity of the supplier as there is not much trust at this point. The merchant seeks information about prospective purchasers of their goods and services. The merchant at this stage advertises the products and services offered to grab the attention of potential buyers. This is where marketing techniques are used by the merchant. In the case of a digital product, the merchant addresses issues relating to copyright and obtains

rights and/or permission from the producer of the product to enable him/her to sell these without any legal issues arising. (Clarke, 2000)

(2) The Contractual Phase

During this phase, a formal relationship is established between the buyer and the seller, including terms and conditions to be applied to any transactions (under the contract). This details the laws and regulations that would be followed and any special conditions that might apply; the steps that would be taken in case of dispute, as well as the policies and procedures, are outlined in this phase. This phase also details the negotiation procedures between the two transacting parties (Clarke, 2000).

(3) The Ordering Phase

Now, the contract has been laid out, and the next step involves the actual placement of an order, or in e-commerce terms, placing the offer. Once the offer is made, it is accepted and acknowledged by the other party (generally the merchant). Once there is an acknowledgement on the part of the merchant, this indicates the preparedness from the merchant's end to deliver the product as stated (this is referred to as acceptance in e-commerce). There are possibilities whereby there could be amendments made to the existing order (cancellations, renegotiations, etc.) (Clarke, 2000).

(4) The Logistics Phase

This stage describes how the actual delivery of goods and/or the performance of services would take place, despite the order having to take place over the Internet (using various technologies). This phase deals with the physical delivery of products and services. In addition, there are also some post-delivery functions that could be involved in this phase in relation to inspection of the goods or services delivered, and acceptance or rejection of the goods from the customer's end (Clarke, 2000).

(5) The Settlement Phase

This is a key phase whereby the goods or services are paid for by the customer. This pivotal phase includes the involvement of financial institutions, such as the Financial Services Authority (FSA), which would assist in the provision of effective fund transfers between the parties, by

confirming any transactions that affect the relevant accounts, and also by confirming any balances as well as the identities of the parties where relevant and necessary. The transactions involved in this phase include those that revolve around payments such as invoicing, payment authorisation, actual payment, and remittance advice transmission (Clarke, 2000).

(6) The Post-Processing Phase

The basic transaction phase is complete at this stage. However, not all the phases and activities are complete. There are a number of additional activities that could be pending, which might include management of information and reports et cetera for the merchant. In certain cases, there could be a statutory obligation to report data or statistics to industry associations or other legal authorities and/or the government. There might also be an extended relationship resulting from the sale; this could include value-added additional services such as servicing, extended warranty, maintenance, upgrading, etc. This phase involves all those additional activities that are not covered in the other e-commerce transaction phases (Clarke, 2000).

Rolf Wigand (RT Wigand, 2006) describes e-commerce as a relatively new concept that began only a few decades ago (somewhere around 1970). He describes how the concept has evolved and discusses in detail the contributing factors, the market drivers and the evolution of the technology and the Internet. This publication further discusses the theoretical and conceptual approach to e-commerce.

3.1.1 Components of E-commerce

Zhang (Zhang Qin, 2009) in his book discusses e-commerce in detail, including its components, technologies, etc. ISO (International Standards Organisation) defines e-commerce as the *"general term for exchange of information among enterprises and between enterprise and customers"*. This definition however does not give a holistic meaning to the actual term. E-commerce nowadays is more than just the sharing of information between parties; it is a business enabler and consists of a great many underlying technologies and components, designed to enable the smooth flow of any related information between these parties.

The key e-commerce components as described by Zhang are shown in Figure 3.3. As depicted, e-commerce involves not just the transacting parties but also relies on other parties, such as the bank, Trusted Third Party and/or Certification Authority (CA), etc., to ensure seamless transactions and also assist in the provision of security and privacy and/or anonymity. Provision

of trust is not an easy task, and is considered a formidable challenge, particularly in the e-commerce arena.

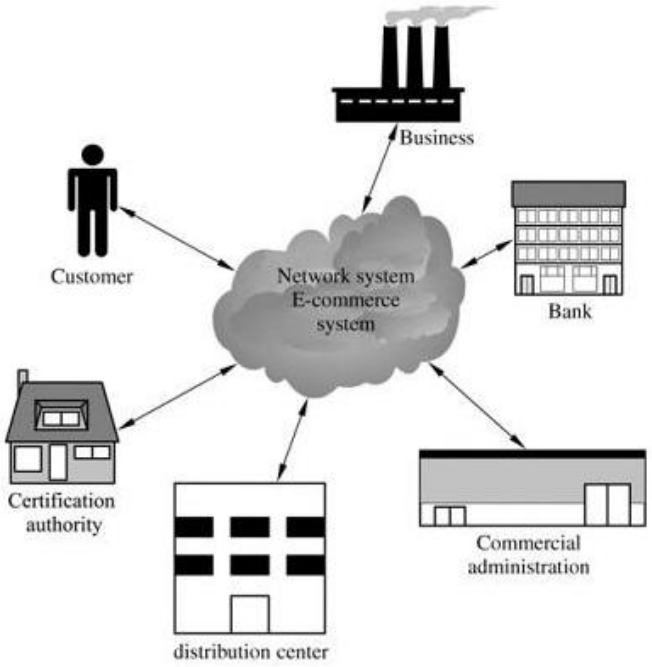


Fig. 3.3: Components of e-commerce

Figure source: Z Qin, 2009

3.1.2 E-commerce Types

E-commerce can be broadly classified into different types depending on the entities involved in the transaction (for example between businesses or individuals). The different categories are Business-to-Consumer (B2C) where e-commerce transaction that takes place between a business organisation and any individual customer, for example, a transaction takes place online, where a merchant displays products to sell and a customer buys those products, as one does in a traditional marketplace, Business-to-Business (B2B)where an e-commerce transaction takes place between two business organisations, for example, one business can purchase raw materials or other products from a different business online for the purpose of developing a new product or for reselling,Consumer-to-Consumer (C2C) where one individual customer sells products and/or services online directly to other customers requiring the products and/or

services and Consumer-to-Business (C2B) whereby a customer uses the Internet and/or telecommunication technologies to sell products and/or services to business organizations (Gefen, 2000)

3.1.3 Advantages, Disadvantages and Restrictions of E-commerce

Having understood the definition and types of e-commerce, the aim of this section is to highlight the various advantages, disadvantages and restrictions e-commerce might have.

3.1.3.1 Advantages of e-commerce

E-commerce changes the way businesses operate and has had a major impact on the way that business is conducted; it is now a key driver that enables businesses to rethink their business strategy and business operating model. This paper earlier discussed the advantages of e-commerce from the point of view of the customer. This section concentrates on describing the advantages of e-commerce to the merchant.

The various advantages of e-commerce are as follows :

1. In simple terms, it enables the owner/manager to increase the profitability of the business and to reduce costs (Min & Wolfinbarger, 2005).
2. It allows businesses to reach out to different customers across the globe.
3. It enables the creation of virtual communities that can be an ideal target for certain specific types of products or services (G Schneider, 2010).
4. It increases the speed and the efficiency at which information is stored and processed (Patil et al, 2014).

3.1.3.2 Disadvantages of e-commerce

As with any product, service or technology, e-commerce has disadvantages, some of which can be critical. These disadvantages sometimes become a bottleneck forcing the businesses to constantly upgrade technologies. There are certain other issues, such as trust, transaction security, data protection, etc., that can be a major challenge to a business, particularly as e-businesses are required to comply with various laws and regulations, including data protection regulations. There is also a concern relating to the particular legislation that must be invoked in any dispute resolution, which forces both the merchant and the customer to clearly understand the contracts and legalities associated with purchasing or selling online, especially across

borders. This section describes the disadvantages of e-commerce both to the customers as well as the merchants.

The major disadvantages relating to e-commerce are as follows :

1. It is not possible to adequately inspect certain items, such as foods that are perishable, jewellery that is custom-made, etc. The underlying technologies do not provide the means to inspect goods although they can ensure delivery of goods (G Schneider, 2010).
2. E-commerce technologies are rapidly developing and this makes it challenging for both merchants and customers as there is a constant need to upgrade. However, this should soon fade as e-commerce becomes more mature (Patil et al, 2014).
3. From the point of view of the business, it is very hard to commit to investing technology, as it is difficult to calculate returns-on-investment, especially if the business is entering the e-commerce arena for the first time (Min & Wolfinbarger, 2005).
4. Businesses face cultural and legal issues while conducting business online.
5. The legal environment in which e-commerce works is not very clear, due to overlapping laws and legislations in different parts of the world (Min & Wolfinbarger, 2005).

3.1.3.3 Restrictions of e-commerce

Though e-commerce enables the availability of goods and services across the globe, there are certain factors that restrict e-commerce transactions from taking place smoothly. These pose as restrictions and can either be legal, ethical or social issues which prohibit business from taking place either in certain industries or regions.

These restrictions include the following:

1. Legacy laws and regulations: in certain industries or geographical regions, laws inhibit e-commerce, forcing businesses to pay penalties for shipments of certain specific goods and/or services in certain industries or in specific regions. This could be because of the fact that many of these laws were developed before e-commerce came into vogue, and hence there might be a different distribution/administrative system through which the merchant is required to pass in order to conduct business (R T Cruz, 2003).
2. Economy: certain economies that are not liberalised do not promote the buying or selling of certain goods or services, and may subject some to a ban. This leads to a

bottleneck as businesses cannot operate within these economies (Min & Wolfinbarger, 2005).

3. Cultural, social and ethical factors: there are various cultural and social factors that can prove to be difficult while conducting business globally. These could prove to be a hassle as certain products might not be appreciated by consumers in certain areas due to the underlying cultural and social factors affecting the same. Also, depending on the cultural and social values, and on changes in ethics and perception, market penetration in certain countries can be tough (Patil et al, 2014).
4. Government support and the legal system: some governments have unnecessary restrictions on e-commerce, thus making the legal system an entry barrier; improper and unclear legal frameworks make it very difficult for businesses to penetrate a new market (C L Mann et al., 2000).

3.1.4 E-commerce Trust

Prins (C Prins, 2002) describes the different aspects that encapsulate trust. Trust deals with *the belief, or willingness to believe, that one can rely on the goodness, strength, and the ability of somebody (the seller or the buyer) or something (for example Information Technology applications).* The author argues that it as an indispensible element in an e-commerce environment, as the only contact between the buyers and the sellers is through the networking medium, and there is no other means to build a personal relationship (unlike in traditional commerce).

The author (Princs, 2002) further describes how trust can be viewed from different perspectives, and that it takes various forms, including trust in technology, trust between trading parties, trust in the system, and so on. Apart from trust in the communication channel and in the transaction medium, there is a huge risk in terms of trusting the parties involved in a transaction. It is risky because there is no guarantee that the goods will be delivered on time or that the goods ordered will be the same as the ones delivered. Similarly for the merchant, there is a trust issue in terms of receipt of payment.

The author (Prins, 2002) describes how trust can be improved with the help of legislation designed to ensure that the honest party is not liable for any dishonesty on the part of the other party. Such legislation should protect the interests of those customers and merchants who have no intention of cheating or being dishonest during a transaction. From a psychological point of

view, the author discusses how trust can be improved for customers by making changes to the User Interface Design and by improving the Human Computer Interaction (HCI) factor. From a technical point of view, trust can be improved greatly by means of cryptographic mechanisms (such as digital signatures, hash functions and time-stamps) to improve the level of authenticity and also to ensure the confidentiality and integrity of the data as well as of the entire transaction.

The issue of trust therefore spans a great many different areas and has a serious impact on the business, legal and technological domains. It provides a variety of opportunities and challenges and needs to be handled carefully by businesses. Businesses also need to understand the different perspectives and be able to identify the key components of trust, and to understand the differences between trust in a traditional environment and an electronic environment to be able to effectively handle the issue (Min & Wolfinbarger, 2005).

In many day-to-day circumstances, people place trust in a variety of entities, events, products, belief systems, services, et cetera (Prins, 2002). However, the Internet being a very unfamiliar environment, placing blind trust in it becomes almost impossible. It is critical yet difficult for one party to establish that trust in an e-commerce environment. Trust, in an e-commerce scenario is established in a different manner, unlike in traditional commerce, as relationships are shorter and most of them are transaction-oriented. Furthermore, e-commerce is more impersonal and the scope for committing fraud and abuse is high. It is automated and provides fewer opportunities for the transacting parties to gain a sensory cue to evaluate the other party, as would be the case in traditional commerce. Research has shown that the two critical factors that impact on trust are credibility and benevolence. Benevolence refers to the fact that the one party trusts that the other has good intentions and, whether or not there is a contractual obligation, the party would act in a favourable and reliable manner. Credibility on the other hand, refers to the belief that one party has in terms of the other's expertise to complete the task at hand effectively, efficiently and reliably. Therefore, trust is a dynamic process that would either be enhanced or lowered based on experience. For example, in eBay, depending on the past experience with a vendor, the customer's trust in the vendor might increase or decrease and vice versa. Initially, if trust is established, when expectations are met, trust is not only reinforced but also enhanced (Roy et al., 2001).

The spectrum of the term 'trust' and its relevance in the e-commerce environment is huge. It can be analysed from various angles and various domains and disciplines. There is already a great deal of research being conducted on specific domains and/or disciplines as well as into enforcing trust in e-commerce transactions. However, the scope of trust in this paper is henceforth restricted to the trust between two mutually distrusting parties in an e-commerce transaction, namely the merchant and the customer. The paper discusses various mechanisms that could be used to induce or enhance the trustworthiness of the transacting parties and also to incorporate honesty and integrity into the transacting parties' actions. Henceforth, the type of trust discussed in this paper is strictly restricted to the trust between the merchant and the customer, or the trust that both these transacting parties place on an unbiased arbitrator, namely the Trusted Third Party (TTP) (Prins, 2002; Roy et al., 2001).

There are various trust models that use various factors, such as familiarity, credit-history scoring, fuzzy logic, and reputation-based trust, which are used by both the merchant and the customer to evaluate the trustworthiness of the other party. One author (Li et al., 2003) summarises the key parameters of trust for reputation-based systems (e-commerce systems that utilise feedback and the past experiences of the parties involved in the transaction to determine the trust levels). These parameters, as noted by the author and that are specific to reputation-based trust systems, and includes feedback relating to satisfaction levels, number of transactions, credibility of the feedback, the transaction context factor and finally the community context factor (Li et al, 2003)

The following diagram (Fig. 3.4) shows an online trust model that focuses on the customer's position as well as the different phases of the trust lifecycle (Head M & Hassanein K, 2002).

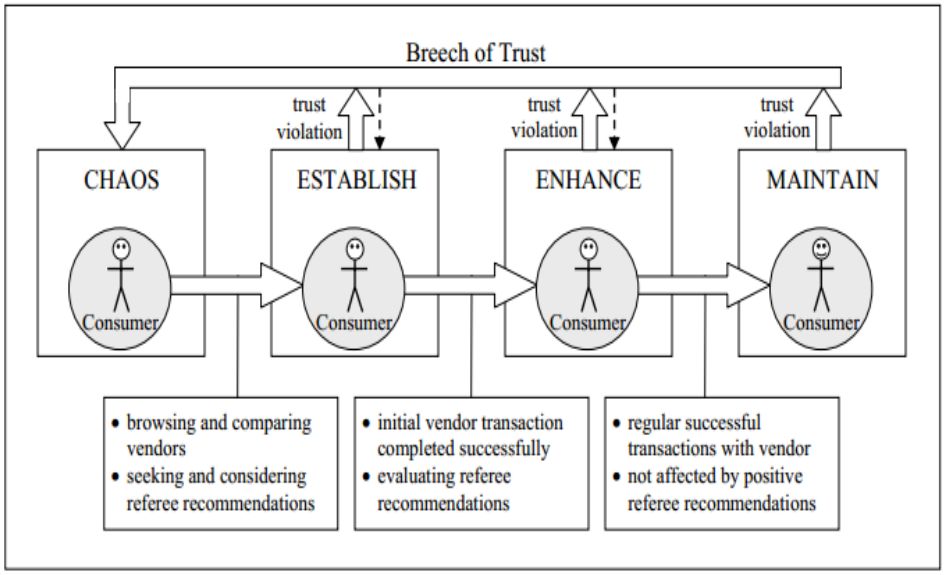


Fig. 3.4: Phases of trust lifecycle

Source: (Head M & Hassanein K, 2002).

The quality of the data that are presented in an e-commerce website also increases or decreases the level of trust in Business-to-Consumer (B2C) websites. Various models have been used to evaluate the quality of such data and to help identify any vulnerabilities in the websites. Identifying vulnerabilities helps the affected business to take appropriate action in order to ensure that the threat does not materialise. One such study (Al-Dwairi & Kamala M A, 2010) proposes a model to identify vulnerabilities and to evaluate the quality of the website; it is based on four key quality factors, namely security, privacy, design and content. Taking into account only these four key quality factors assists in reducing the huge amounts of data that would be needed for testing in some other models. Another research also stresses the importance of having an integrated trust model and discusses about how trust could be perceived from different perspectives, such as economic, social, psychological, organisational or technological. Given the various perspectives associated with trust, it is difficult for businesses to implement trust, and thus there arises a need for an integrated point of view to help implement the key elements into electronic commerce websites (Al-Dwairi & Kamala M A, 2009).

Trust therefore plays a pivotal role in e-commerce and it is imperative that businesses ensure that their customers' trust is winnable. Businesses need not only to be able to understand the

effects and impact of trust on business success and but also be able to adapt to the changing perceptions and technologies.

3.1.5 E-commerce Architecture

There are various components that encompasses e-commerce technologies and it is not just confined to the web portal. These components are built together to provide a variety of services in the e-commerce architecture and acts as an enabler to e-commerce websites. These technologies include but are not limited to Extensible Markup Language popularly known as XML, standards such as Secure Electronic transactions (SET), Open Buying on the Internet (OBI), et cetera. Researchers believe that it is key to be able to embody the needs of the business architecture within the technological framework and components (F Hoque, 2000).

These technological components that are a part of the e-commerce technology framework are used to provide seamless communication and secure channels that facilitate the provision of user-friendly websites to customers. The various components that act as enablers are the underlying e-commerce software, infrastructure including server software, hardware as well as the server-side operating system. (R M Stair et al, 2012). These are depicted in Fig. 3.5

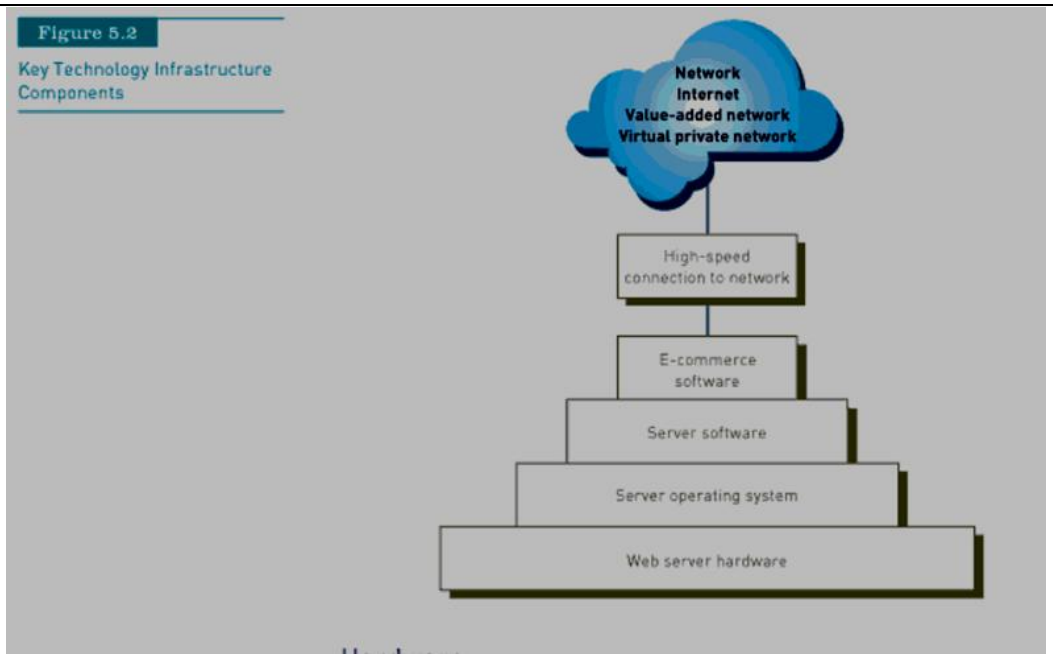


Fig. 3.5: Key components of e-commerce infrastructure (R M Stair et al., 2012)

Source: R M Stair et al, 2012

3.1.6 E-commerce Risks

It is key to understand what a Risk is. Risk according to ISO/IEC Guide 73 (ISO/IEC Guide) has been defined as the probability of an event occurring along with its consequences combined. It can also be defined as the uncertainty of an event occurring be it positive or negative in terms of project management (SANS Institute, 2008 525.5 2-5). Understanding what impacts the risk has on a business is assessed by performing a risk assessment. In the global technological age where everything is digital all business organisations rely on the use of Information and Communication Technologies to facilitate automation of business processes (Computer Systems laboratory Bulletin, 1994). Risk Management in IT enables to identify the key risks, assess the same for the impact it would have on the business, prioritise the risks based on the probability and impact it would have on the information assets of a business. It also facilitates the constant monitoring and controlling either the occurrence of the risk or mitigating the impacts it would have within a business environment (Hubbard, 2009). To enable mitigate losses that might arise out of the risk materialising, it is imperative for the business organisations to identify, evaluate and have an effective risk management strategy and framework for monitoring, recording and reporting risks. Risk management strategy thus enables the business to have a better understanding of the threats that they might be facing and come up with effective and efficient strategies that would help countering these threats and avoid losses. It also paves way for the businesses to be prepared and accept the risk where unavoidable.

Electronic business and e-commerce pose may threats and risks to a business, as much as the opportunities they offer. Chaffey (D Chaffey, 2011) discusses the risks to business while implementing e-commerce; these include both strategic and practical risks. Strategic risks to business could range from poor business decisions that lead to a collapse of the business, improper planning and management of e-commerce strategies, through flaws in executing the right technological solutions (which can lead to additional costs), to inappropriate investment strategies that makes it impossible for the business to gain what it hoped for.

Apart from the strategic risks, there are various other risks that merchants as well as customers face on a day-to-day practical basis. These risks could be any of the following:

1. Sudden decrease in customer traffic due to various external elements that had not been factored in. For example, there could be a sudden decrease after the end of an advertisement or a roll out campaign (Hubbard, 2009).

2. Websites always face the risk of being hacked, which might lead to loss of reputation, financial loss and in certain cases also act as a threat to the legal compliance of the business (Li et al, 2002).
3. Fulfilment of orders in a timely manner is always a challenge, as it is based on external entities that are not directly related to the business. There is heavy reliance on the supply chain, which might be affected or compromised. Hence this could result in the delay of goods and/or services being delivered at the right time, leading to loss of trust in the customer (Chaffey, 2011).
4. Customers face the risk of being contacted by the company or the merchant by receiving constant unsolicited emails or the threat of being constantly harassed with spam mails.
5. There are problems relating to identity theft, whereby the customer's personal information is stolen and used for illegal purposes.
6. Should a problem arise, the customer's emails may not reaching the appropriate contact due to network, server or system errors, thus leading to a dissatisfied customer.

(Chaffey, 2011)

From the above, it is clear that there is a fundamental difference between traditional business risk and e-commerce risk. The latter varies in terms of scope, size and nature, and the fact that the risk spans across countries. There is also a difference here as the e-commerce market is not as mature as the traditional marketplace; it is constantly evolving and will take a few more years to stabilise and become sufficiently mature for businesses to easily predict risks and to decide on the risk strategies.

Another author (Panko, 2004), while discussing risk, stresses on having a formalised process for risk management strategy and to ensure that this strategy that has been developed keeping in mind the business strategy. The author says that not only is it essential to have a well developed risk strategy but it is also key to ensure that all business processes are aligned to this strategy. While implementing e-commerce solutions there are various risks that businesses might face .

DoS Attacks: Denial of Service is one of the major risks that businesses can face. This attack stops legitimate users like the business as well as the customers from being able to access services at the right time (Panko, 2004; Chaffey, 2011).

Intrusion attacks: In these attacks, the customers' data or the database that holds this information is attacked. This type of attack is performed to obtain Personally Identifiable Information (PII) or other sensitive information held by the system which could potentially lead to greater thefts and losses (Panko, 2004).

Identity theft: Following intrusion attack, once the PII is obtained by the attacker, this might lead to identity theft as there is a huge volume of data that is held by the servers and e-commerce systems (Panko, 2004).

Malware: this includes viruses, worms, Trojan Horses and any hybrid malwares that target the system or the network with the aim to damage the data or for other purposes like relaying information, stealing data et cetera (Hubbard, 2009).

There are thus various ways of managing the risks; they can be tackled depending on the dimension or the processes they occurs in. This can be classified into: risks in services, risks in business models, risks in technology, risks in processes and risks in fulfilment. Once the risk and its dimensions are identified, it is important to then understand the legal approach that must be taken to manage the e-risk (J Sounderpandian, 2007).

3.1.7 E-commerce Security

From the above it can be understood that there are various ways in which the e-commerce systems can be targeted by attackers. Hence security plays a major role for e-commerce websites. It is essential to have a security strategy implemented to be able to counter these threats and also to provide a safe environment for the customers that would increase their trust in the business. To be able to do this, businesses would first have to identify the areas of concern and also the security needs for the technology as well as the business as a whole.

From a technology point of view, a web server that is secure has to be first obtained based on the needs and wants of the business. Before procuring the server, it is essential that the business is aware of the costs, functionalities provided and the security support the server can offer. It is also important to assess whether the server would be able to handle various security protocols such as the SET. Next various authentication mechanisms should be implemented and it is essential that the administrators define the rights, permissions for various users and the server should be hardened. While doing all this, the business should also take into account the

compromise on speed and should be able to decide on an optimal security software and speed capacity limit. Encryption mechanisms should be followed while storing passwords for various databases and industry best practices needs to be followed. Based on the authentication and user level permissions, the web server should be capable of displaying or hiding certain pages to the end user (R Russell, 2001).

Another key issue is being able to offer transactional security by e-commerce technologies. These include origin non-repudiation, payment receipts, submission times and care should be taken to host the website on a secure platform. Being compliant with various rules and regulations is also key. There are various acts and regulations such as the Data Protection Act of 1998 the Copyright Designs and Patents Act 1988, the Privacy and Electronic Communications Regulation 2003, that businesses need to adhere to. Similarly to conduct an online business it is also important to follow financial standards like the PCI/DSS (Payment Card Industry) (A Calder, 2006).

Anup Ghosh (AK Ghosh, 1998) discusses the various vulnerabilities, threats, risks and security issues relating to e-commerce. He further addresses securing the various components of e-commerce architecture. The various key threats to e-commerce include Vandalism and sabotage on the Internet, Breach of privacy and/or confidentiality of data,Theft and fraud, Issues relating to data integrity, DoS attacks that lead to a situation whereby the organization is unable to conduct its business online for a while until they are able to resume activities on the server (Ghosh, 1998).

According to the author, it is important to take into account the entire architecture (system-wide security), including Client security, Transport security, Server security, including all web applications and database servers, Operating System security, Application security, Payment system security, Communication channel security, using HTTP over SSL (HTTPS), Gateway and script security, to prevent malicious software or scripts from being executed (Ghosh, 1998)

The author discusses building trust in detail, through making use of appropriate authentication and authorization mechanisms and exploiting cryptographic techniques to ensure that the entire e-commerce architecture is protected from both the client end as well as the server side. Careful coding, effective testing and using secure coding practices can avert a great many threats and

can prevent attacks caused due to malfunction or poor code, such as buffer overflow attacks, cross-site scripting attacks, SQL injections, etc (Ghosh, 1998).

E-commerce technologies are susceptible to vulnerabilities and threats. From a technological point of view, e-commerce transaction security includes the usage of digital signatures; using a certificate authority (CA) ensures that certification policies are adhered to and that the digital signatures do indeed help in verifying the identity of the parties involved. E-commerce transaction security also entails the usage of appropriate end-point and network security solutions, such as firewalls, VPN's (Virtual Private Networks), email security, web security, et cetera.

From a business and legal point of view, it is important to have appropriate technical security policies and procedures; these need to be adhered to, and the Public Key Infrastructure must be understood for it to be implemented effectively and efficiently. Cross-border regulations must also be adhered to, and it is imperative for the business to thoroughly understand the various data protection laws and regulations (W Ford et al., 2000).

Total security can be provided when there is care taken to protect all the platforms and the information assets. One of the key security threats is transferring data over wireless channels and this can be countered if the business has a good policy that would help protect the wireless communication channel and media. Various key technologies are involved in ensuring the success of the e-commerce platform and businesses need to have a thorough understanding of this. It is not just enough to buy security solutions off the shelf without performing adequate research on the needs of the business and also getting an idea of the different key vendors in the marketplace and their service offerings. It is important that the business is able to map the requirements to the service offerings of the vendors and make an informed choice of the vendor as well as the security solution. Furthermore, the businesses can also be protected from other liabilities and risk can be transferred to third parties by having good Service Level agreements (SLAs) with the parties concerned. This acts as a legal binding between the parties and the business can enforce legal action when the contract is breached. (SANS reading room, 2012).

Another author (V Hassler, 2000) discusses the various attacks that are possible in an e-commerce environment that might jeopardise the entire system and/or the data. These attacks could range from any of the following but is not limited to the following.

Eavesdropping: in this type of attack, the attacker intercepts messages by constantly monitoring and reading messages meant for other parties (Ford et al, 2000).

Masquerading: here the attacker uses a false identity to send and/or receive messages (SANS reading room, 2012).

Message tampering: this is more than eavesdropping, where the attacker not only reads the message but also alters the same (Hassler, 2000)

Replaying: in this type of attack, the attacker uses one of the old messages sent between two parties to gain certain privileges. Infiltration: abusing the authority of a legitimate user, the attacker gains entry into a system to run a malicious program in order to compromise the system and/or steal data. Traffic analysis: here the attacker monitors constantly the packets of data that are sent between two parties. It is a passive attack whereby the attacker limits himself to only analysing the packets. Denial-of-Service (DoS): the attacker does not allow legitimate and authorised users to use the system and its resources (Hassler, 2000).

The various security services that are key to any system and also to an e-commerce system, as described by the International Standards Organisation, include Confidentiality, Integrity and Availability:

Confidentiality

Data that is stored needs to be kept confidential and should be available only to users who have the rights to view it. Confidentiality ensures that illegitimate or unauthorised users do not have access to the data that is stored on the databases or any other systems. Traditionally, confidentiality has been achieved by businesses by having access rights that would allow only certain specific users to view or modify data based on their privileges granted by the system administrator and controlled by means of using a username and password combination (SANS reading room, 2012).

Availability

E-commerce websites are built with the idea of providing a 24/7 service to customers across the globe. Different people would make purchases at different times and it is therefore essential to ensure availability of the website and the data to legitimate users at any given point in time. Unavailability leads to financial loss to the business as every minute of downtime would mean

loss of revenue. Also, given the competition in the market, customers might not prefer to use the website again if it has a lot of downtime as there are various other vendors that would provide similar products at competitive prices. To avoid unavailability for longer periods of time, businesses should have a good back up policy that would help resume the system and make it up and running even within short spans of time (SANS reading room, 2012)

Integrity

While confidentiality ensures that only legitimate users have rights to access the data, integrity ensures that the data that the business holds is exactly the same as the one entered by the customer. It means that the data has not been tampered with and that no unauthorised or even authorised resources can make illegitimate modifications to the data intentionally or by accident. Businesses make use of firewalls that would harden the data servers and also ensuring that secure methods are followed while redirecting from and to the payment gateway channels. Integrity provides reliability and also ensures that the data held by the business is up-to-date and constant across different databases (SANS reading room, 2012).

Non-repudiation

Non repudiation of origin, transactions, purchase , payment, receipt is essential and e-commerce technologies should be able to provide this service. It helps to ensure that the person or the entity performing certain specific actions cannot at a later stage refute the actions for any given reason (SANS reading room, 2012; Ford et al, 2000).

The author (Ghosh, 1998)describes the key security mechanisms for e-commerce that could be used in order to implement the security services mentioned above. These security mechanisms also help combat any attacks to the e-commerce solution. These include the following:

1. Encryption mechanisms that help protect confidentiality.
2. Digital signatures, which verify the claimed identity of the party.
3. Access control mechanisms, to help prevent attacks that arise out of unauthorized access and also to assign permissions for different entities.
4. Data integrity mechanisms, to avoid data manipulation and message tampering.
5. Authentication exchange mechanisms.
6. Traffic–padding, to stop message replays and traffic analysis.

7. Routing control mechanisms, to help send data only through trusted nodes.
8. Notarisation mechanisms, to make use of a trusted third party notary that can be used in case of dispute resolution.

3.1.7.1 E-commerce security – users' perception

Perception of trust and security in many cases are driven by the design and the layout of the e-commerce website in the minds of the users or customers. Research shows that this perception of trust and security can be enhanced by the businesses by providing a good design for the interface and also ensuring that the data that is presented in the website is accurate, up-to-date and also correct. Furthermore, following best practices in terms of design and using layouts that customers are used to, displaying information clearly, having a detailed FAQ section and providing ease of navigation enhances the perception of security in the users' minds. (F Kamoun et al., 2012)

Similarly other studies also show that the concept of a good interface design is pivotal in increasing the perception of the security offered by the website and this includes integrity perception, privacy control perception and the overall system security perception. (M Chaisson et al., 2011)

3.1.7.2 Data quality & security

Data quality has a major role to play in the provision of good security of the system. It is not just enough to have good technologies but these needs to be backed up by good data quality policies. Documenting and enforcing policies ensures that the data that is held is consistent while being stored, transferred or transmitted even over insecure channels. This policy should also specify instructions about the backup of data at regular intervals, data access mechanisms, policies and rules. Analytics that are performed on date help businesses gain an understanding of various customer preferences and it is therefore necessary that the data held is accurate as inaccurate data would lead to gaining false business insights. The most recent data backup should be identifiable and also reliable and the business should be able to access these immediately in case of any data issues. Understanding the drawbacks of data loss, data leakage and data unavailability would ensure that the business policies are written and enforced to take into considerations these factors and help profile data in an effective and accurate manner (Kamoun et al., 2012) .

Data owners and access control techniques and methods should be used to ensure that the data held is kept confidential. Classification of data also helps to make sure that unauthorised entities or those entities that do not need the data is able to gain access to it. These policies relating to data cleansing, integrity, storage and backup should be addressed in the security policy and aligned with the business strategic policies and goals and should remain consistent across the business (M Chaisson et al., 2011).

3.2 Trusted Third Party

Trusted third party (TTP) can be defined as *"an entity in a domain that is trusted to perform a specific service"* (Springer Reference, 2013).

A Trusted Third Party enables transparent, seamless transactions to take place in an e-commerce scenario. The TTP emanates from the need to quantify and account for the transactions as and when they occur electronically (L Columbus, 1999).

One research (J W Palmer et al., 2006) talks about the role of Trusted Third Parties and other intermediaries in the critical development of an e-commerce business. It describes a TTP as *"one set of organizations that try to promote trust on the Web. A TTP will display its logo on a firm's web site if that firm has demonstrated that it conforms to the policy of the TTP."* Some of the most trusted third party organizations include TRUSTe, BBB Online & VeriSign. From the customers' point of view, the intermediary or the TTP acts as a guarantor, where they can place trust in its integrity. Many Internet vendors make use of the TTP to answer strategic business questions and also to increase customer confidence by building a trusting relationship.

In a paper by Jonathan et al. (Jonathan et al., 2006), the authors describe the importance of establishing trust between the suppliers and the consumers (merchants and customers) and argue that it is critical for the continued growth of e-commerce. To establish this trust in customers, a TTP plays a major role. In simple terms, it could be one or a set of organizations that display their logo on the webpage to ensure the customer that the website is highly trustworthy and that it follows certain principles and conforms to various compliance policies. The TTP in this case acts as an intermediary between the merchant and the customer.

Cryptography plays a key role in the establishment of trust in e-commerce. For secure electronic transactions, most cryptographic protocols make use of a separate party that is unbiased, known

as the Trusted Third Party or TTP. The TTP can be any organization or in certain cases individuals such as banks, financial institutions or Certificate Authorities (CA). For example, the Certificate Authority would verify the link between the said individuals and their identities by making use of their public keys. The TTP would not vouch for the trustworthiness of the mentioned party but merely verifies the public key and authenticates the identity of the party (Grandison and Sloman, 2000).

Nenadic & Zhang (Nenadic & Zhang, 2003) defines a Trusted Third Party as *a neutral party (entity) that is used in fair exchange protocols to ensure fairness for all parties involved in the exchange of items. The TTP is assumed to be available, trusted by all parties and not to collude with any party.* The TTP therefore ensures that fairness is achieved in a transaction across all parties, acts as an intermediary and delivery agent that is used to deliver items to the parties, acting as an authority that can validate and verify the identity of the transacting parties, act to resolve any disputes that might arise out of dishonest transactions or misbehaving parties and finally validating and/or issuing certificates where necessary (Nenadic & Zhang, 2003)

Trusted Third Parties are thus entities that are employed in an e-commerce environment to facilitate trust. In traditional commerce, these entities could be anything ranging from lawyers, bankers, financial institutions, brokers, et cetera. In addition to these entities, the new TTPs in the modern e-commerce environment include Certificate Authorities (CA), time-stamping authorities and digital notaries. In a dynamic and ever-changing e-commerce environment, the role of the TTP is constantly evolving and the services offered reflect the paradigm shift in the establishment of trust over the Internet. The author describes some of the key questions that could be answered by using a TTP. These include: Will the authenticity of the other party be verified? The verification of the “claimed identity” is checked. How good is the trustworthiness of the other party? How sure can I be that the communication that has been sent is genuine and not tampered with? Can eavesdroppers be prevented? In case of a dispute, is there any reliable source to provide evidence? (P J Skevington & T P Hart, 1997)

To answer these questions, there are various services offered and different roles that the TTP can play. These roles enable smooth transaction between the two parties by helping authenticate the identities of the transacting parties, check credentials, guarantee the integrity

and confidentiality of any information sent and received, settle disputes, provide a secure communication channel for secure payment.

(P J Skevington & T P Hart, 1997)

3.3 Legal and Regulatory Aspects of E-commerce

E-commerce solutions add a layer of complexity to the business when compared to the traditional marketplace as any person across the globe will be able to access the Internet and there can be threats from any corner of the world. Also, customers can be from any part of the world which means that the business should understand the legal framework and the regulatory aspects of transacting worldwide. Various regulations and legal boundaries pose a challenge to the business and there are various laws and directives that the business needs to adhere to. Similarly there are various international standards that are mandatory to be complied with in order to trade globally and the business needs to be aware of these.

In the UK, the E-Commerce Regulations of 2002 (EC Directive) is a pivotal directive that governs various aspects of e-commerce that the business needs to follow and adhere to. This directive forms a basis that provides guidance on key terms related to the e-commerce marketplace like contract, order, service provider and also gives a detailed explanation of what the businesses need to do to be compliant with the directive. It governs the jurisdiction that would need to be adopted to when there is a dispute, burden of proof in case of criminal court proceedings, the rights and responsibilities of the trading parties, service providers and their liabilities et cetera. (EC Directive, 2002).

The EU directive also governs regulations relating to competition law, describes and details various terms such as the laws in the country of origin of transactions, responsibilities of the network service providers, what and who is responsible for the webpage being hosted, duties of the certification authority, and the legal effectiveness of digital signatures (which is described within the Signature Directive). The Signature Directive describes when and how digital signatures can be used in a court of law as evidence and how digital signatures that are secure could be used as an alternative for handwritten signatures. It also describes in detail competition law, torts, and the contractual obligations of both the customers and the merchants. The EU directive has another directive known as the Distance Selling Directive, which

is provided for the unique protection of the customers of e-business. Other directives within the EU directive include the Data Protection Directive and the Directive on Privacy and Telecommunications, which contains rules on the data privacy of customers and the freedom of customers not to choose to share personal information over the Internet (T Kono et al., 2002).

Blythe (S E Blythe, 2011) explains that the legal landscape as well as e-commerce law refers to all regulations relating to electronic contracts, electronic signature law, certification authority law and regulations, consumer protection in e-commerce transactions and aspects relating to the provision of electronic evidence and processing. The MLEC (Model Law of E-Commerce) was drafted by the United Nations in 1996 to offer internationally acceptable rules and to also enable the provision of a secure environment. It applies to any kind of data or network that is used in the context of commercial activities over the Internet. It acts as an enabler providing a set of guidelines, a framework and principles to facilitate the use of modern technology in business. It acts only as a framework giving every individual nation an opportunity to draft in detail the specific laws and regulations necessary for implementation.

Based on the Data Protection Act, there is a necessity for organisations or businesses to notify the local data authority (the Information Commissioners Office in the case of UK) of any personal data breach within 24 hours of becoming aware of the basic facts. Furthermore, the organisation/business that has reported a breach must follow up with an update within the next 3 days. If a breach is likely to adversely affect individuals, the organisation/business must notify those individuals without undue delay. A personal data breach is defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise protected in connection with the provision of a public electronic communications service*." (ICO, 2013)

Personal data means any kind of information (a single piece of information or a dataset) that can personally identify an individual or single them out as an individual. Examples include vehicle registration plate numbers, credit card numbers, fingerprints, IP address (e.g. if used by a person rather than a device, like a web server), or health records.

The data authority will review the incident that has been reported and decide if any enforcement action is required. For the Information Commissioners Office (ICO, 2013) the options are:

- Penalties of up to £500,000
- Audits
- Enforcement notices
- Prosecution

According to the data provided by the ICO (2013),

- During 2012, the number of organisations that received monetary penalties from the ICO increased by more than 200%.

- Between 03/2011 and 02/2012 there were 730 self-reported breaches and 1,150 in the same months during 2012 to 2013. Over the same periods, the number of monetary penalties imposed increased: from 9 penalties totalling £791,000 in 2011-2012 to 20 penalties totalling £2,610,000 in 2012-2013, a growth of more than 200%. (ICO, 2013)

Given the legal requirements and the stringent rules in case of data security breaches and concerns relating to data privacy, there is now a paradigm shift in the way security is looked at by organisations and businesses. No longer is security just a matter of securing the end points. It is now considered a holistic process and an end-to-end business requirement which is incorporated in all aspects of the business .

3.4 Fair Exchange

In an e-commerce transaction, as in a traditional business environment, there are two transacting parties, namely the merchant and the customer, who possibly do not know each other, and hence there is a lack of trust between these parties. For example, if the customer wants to buy a product online (say a software program or digital music), the merchant needs to receive the correct digital payment for the product from the customer, and the customer needs to receive the right software from the merchant. The customer should not be cheated by the merchant, who either does not deliver the software after receiving the payment or sends the wrong software to the customer, and similarly the merchant should not be cheated without receiving the payment from the customer. This problem is called ‘fair exchange’ and most e-commerce protocols enable the provision of fair exchange, where either both parties receive their products or neither does. Furthermore, there is another problem that fair exchange

protocols tackle, namely dispute resolution, i.e. an online or automated solution when there are disputes arising out of the transaction between the two parties.

According to Ray (I Ray & I Ray, 2002), a fair exchange protocol is defined as *a protocol that ensures that no player in an e-commerce transaction can gain an advantage over the other player by misbehaving, misinterpreting or by prematurely aborting the protocol.* It describes that fair exchange is achieved in an electronic exchange when at the end of the business transaction, each of the transacting parties fulfils its obligations and receives the item expected or none of the transacting parties involved gets anything.

Asokan (Asokan et al., 1997) defines fair exchange as a system *that does not discriminate against a correctly behaving player. As long as a player is behaving correctly, a fair system should ensure that other players will not gain any advantage over correctly behaving players.* It states that no transacting party (merchant or customer) should receive unfair or undue advantage, thus ensuring fair exchange in the transaction. It describes that the transaction between two parties X & Y (the merchant and the customer) should satisfy three main conditions, namely Effectiveness, Timelines and Fairness.

Effectiveness, whereby on correct execution of the protocol both the transacting parties honour their commitments appropriately. In other words it means that both the parties at the end of the transaction or deal receive their items (Asokan et al, 1997).
Timelines, whereby the protocol that provides fair exchange would be executed within acceptable timeframes (Asokan et al, 1997).
Fairness: this refers to the scenario whereby fair exchange is achieved. The paper describes two types of fairness, namely strong fairness and weak fairness. Strong fairness: this is a type of fair exchange whereby on successful execution of the protocol either both the transacting parties receive the goods or neither receives anything. Weak fairness: in this case, either strong fair exchange is achieved or if not the correctly behaving party is able to prove via a trusted third party that the other transacting party has been misbehaving and provides a means for dispute resolution. Though strong fair exchange is a desirable characteristic, it is not always achievable due to constraints of cost and complexity (Asokan et al, 1997).

There are quite a number of protocols that concentrate on providing fair exchange. Exchange of goods and money takes place over the Internet between two or more parties that do not trust

each other, and hence the provision of fair exchange plays a key role in ensuring that neither parties cheat. Fair exchange protocols belong to the group of security protocols that enable better management between the buyer and the seller in an unknown, risky and un-trusted space.

3.4.1 Fair Exchange Categories

Depending on whether or not the protocol involves a Trusted Third Party, fair exchange protocols can be broadly classified into two types:

1. Those that do not involve a TTP and
2. Protocols that involve a TTP

Protocols that involve a TTP can further be classified into three types, namely inline, online and limited use of TTP.

Use of an inline TTP: in this type, the transacting parties, namely the merchant and the customer, send their items to be exchanged to the TTP, who in turn would deliver them to the transacting parties, thus avoiding any direct contact between the transacting parties. This ensures that fair exchange is guaranteed. The disadvantage of this type of protocol is that the TTP sometimes becomes a bottleneck as it must always be available. It also acts as a single point of failure for the protocol, i.e. if the TTP crashes, then the protocol fails, as the TTP cannot deliver the items to the transacting parties (Springer, 2010). Figure 3. 6 depicts this.

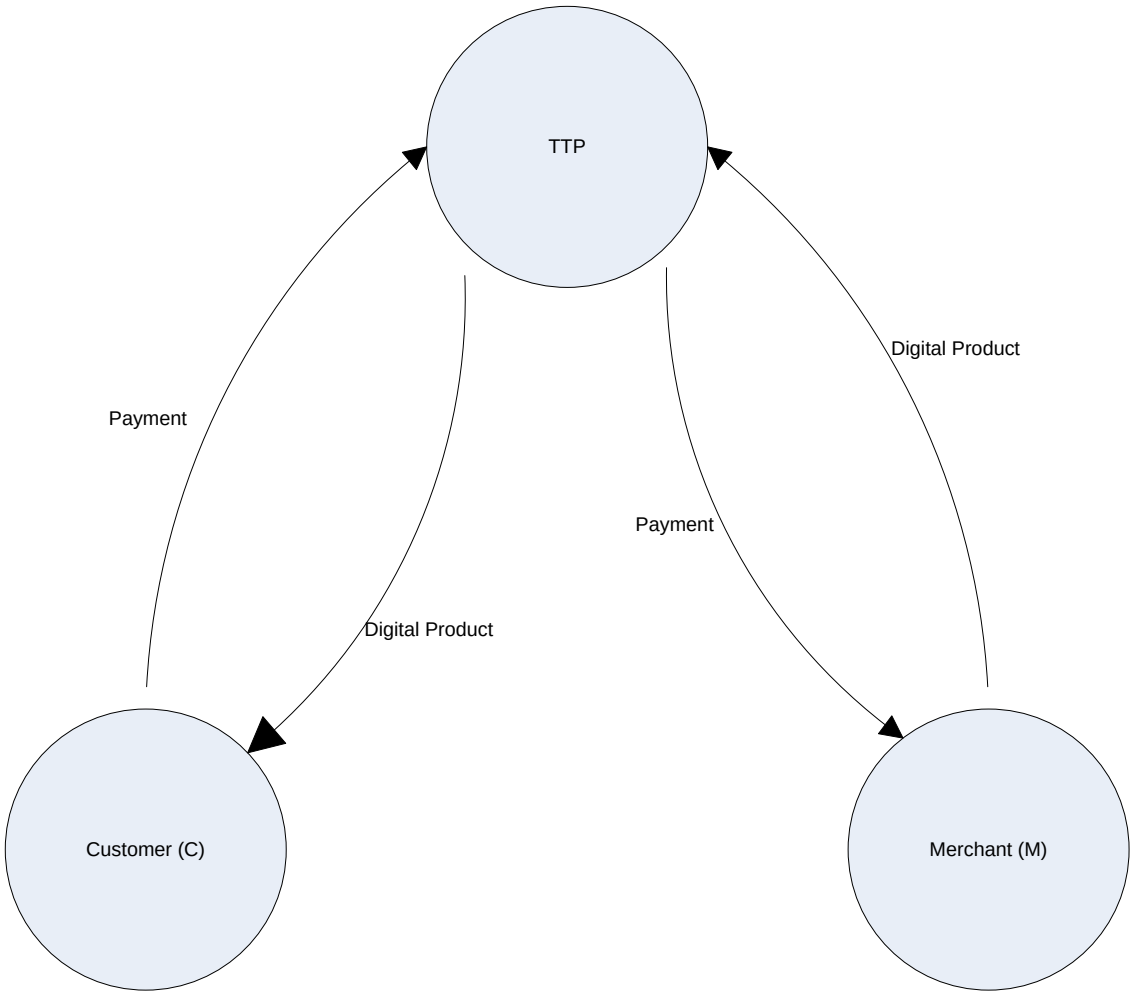


Fig 3.6: Inline TTP based fair exchange model (Springer , 2010)

Use of online TTP: in this type, the TTP is used to validate the items that are to be exchanged. Unlike an inline TTP, an online TTP is used only for validation and hence the involvement of the TTP is slightly reduced. It uses the TTP for the purposes of verifying the items, generating and/or sorting proof of exchange for the times. However, the use of an online TTP also has similar disadvantages (as with an inline TTP) as the TTP needs to be online for the exchange process and also during any disputes that arise. It might also lead to dishonest users or misbehaving parties targeting the TTP to compromise it (Springer, 2010). Fig. 3.7 depicts this in detail.

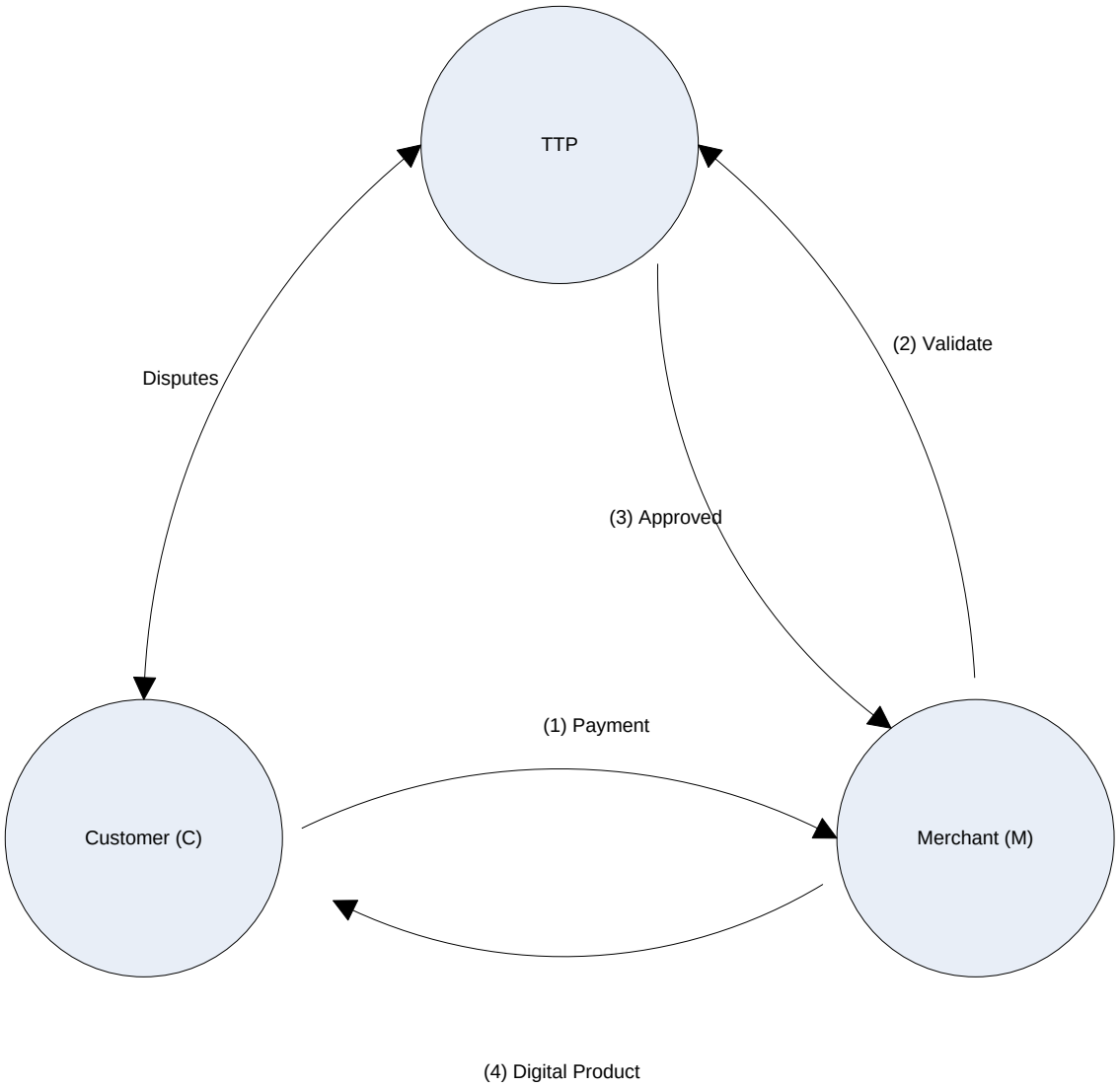


Fig 3.7: Online TTP based fair exchange model (Springer, 2010)

The proposed protocol uses an online TTP model as the TTP helps to build trust between the customer and the merchant. Despite being a bottleneck, it acts as a trusted arbitrator facilitating and recording all transactions which makes it easier to resolve any conflicts if they occur. Also, the TTP verifies that the e-cash and the digital product are valid by verifying it with the bank and the producer respectively. Since there are various benefits of using an online TTP, this research uses this model.

Limited use of TTP: in this type, the TTP is used only when something goes wrong or when a dispute has arisen. This type is called an Optimistic Fair Exchange protocol. Fig. 3.8 depicts this.

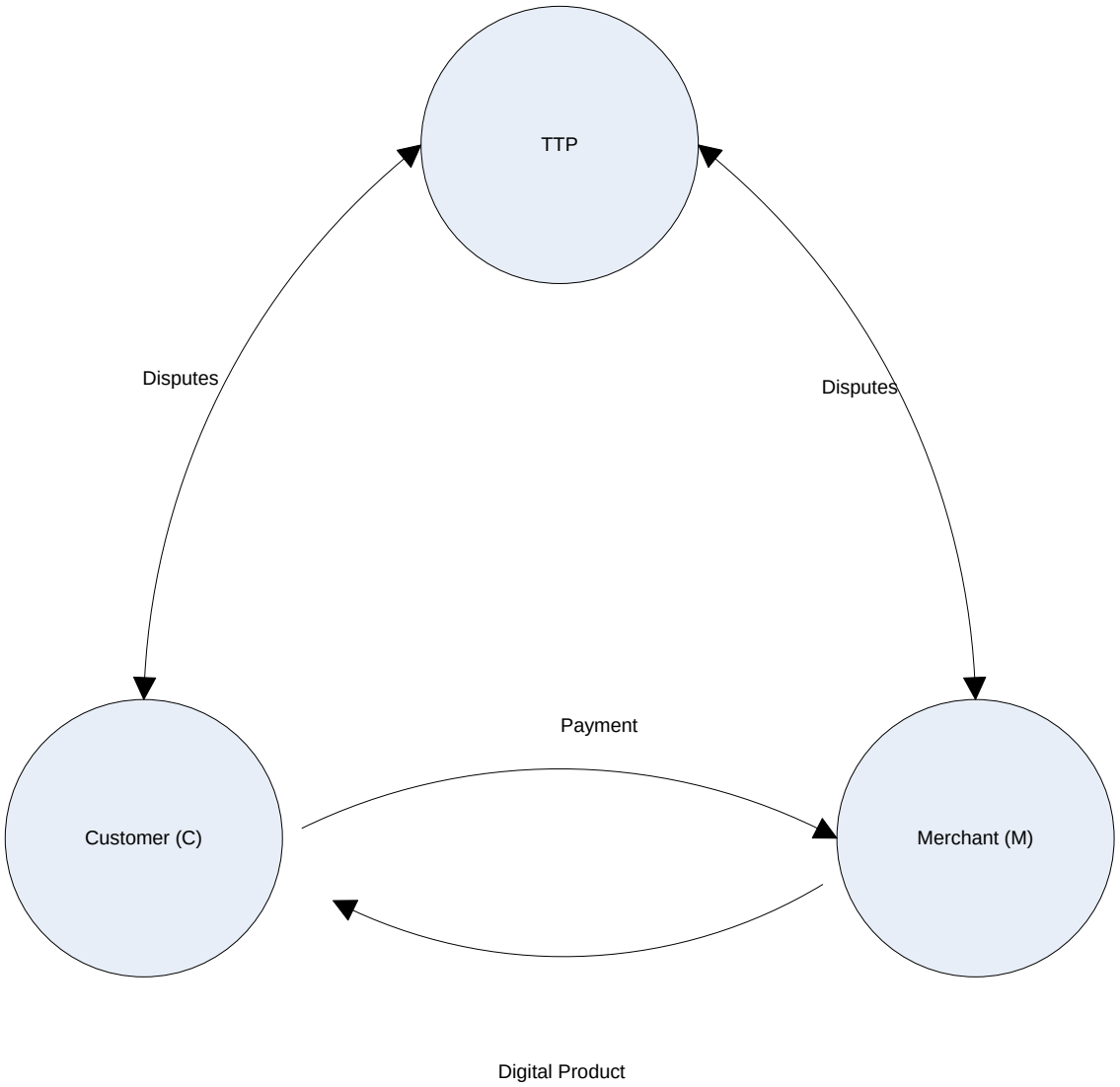


Fig. 3.8: Offline TTP (Optimistic Fair Exchange) protocol model (Springer Images, 2010)

3.5 Data Privacy

The implementation of an e-commerce system brings about a new set of challenges in terms of privacy of data. While a transaction is processed, there is a huge volume of data that is being collected from the customers. A lot of this could be sensitive information including card number and other Personally Identifiable Information (PII) and this makes it mandatory for the business to be able to adhere to the various data protection and privacy rules and regulations (Hines, 2002).

Once businesses decide to implement an e-commerce solution, it is imperative that the business understands that the success of the business is closely related to the level of the trust the customer has on the system as well as the brand image of the business. To be able to build that trust customers should understand and believe that their data is confidential and that there would be no issues in relation to the privacy of information. They should be assured that there would not be any problems that would crop up due to the loss or theft of data and that their personal information will not be mishandled by the business. Data privacy issues can lead to legal complications, and to loss of reputation and finance (Hines, 2002).

Businesses need to understand and appreciate that the privacy of customer data is of huge importance and that they should not be constantly nagged or bothered with emails, promotional offers or offers from other third parties that might not be useful to them. This would lead to the customer being put-off and lose trust in the business. Care should also be taken by the business to constantly be vigilant to prevent data leak and also ensure that appropriate security mechanisms are in place to protect information about the customer that is being held by the business. A customer privacy policy should be formulated and enforced strictly by the business and this policy should be available to the customers to view (M Hines, 2002).

3.6 Anonymity

Anonymity could be defined as *A condition in which an individual's true identity is unknown*. Privacy on the other hand is *A person's right to control access to his or her private data* (Kimpl, 2012).

From the above definitions, it can be clearly understood that anonymity and privacy are not the same and are in fact entirely different things. Anonymity, in the scope of this research, means that the true identity of the customer is hidden. While entering into a contract, the customer does not have any obligation to reveal his or her true identity to the merchant, and there is no way the merchant has the ability to track the true identity of the customer (based on the transaction details). For ensuring privacy of data, various cryptographic mechanisms such as encryption are used.

E-commerce transactions, as discussed, takes place over the Internet where there is no mutual trust between two or more transacting parties. A customer, due to the lack of this trust, would

not want to disclose all his/her details during a transaction. This is achieved by making use of electronic cash that helps to provide transaction anonymity to the customer. Anonymity is thus a mechanism that hides the identity of the customer and keeps it secret during an e-commerce transaction. It helps protect the customer's privacy. Though privacy is an ancient concept, with the development of more technologies, this is yet to achieve its full potential.

3.7 E-Payment

Margaret Tan (M Tan, 2004) defines e-payment, in simple terms, as a process in which monetary value is transferred electronically or digitally between two transacting or entities, as a compensation or consideration for the goods purchased or services obtained. The entities referred to here could be a bank, business, government or any individual customer. This definition explains that any payment that has been made (which is not effected by paper-based instructions such as cash or cheques) and that is done electronically through the use of technology (such as payment cards, store value cards, GIRO instructions, ETF or virtual or digitised money) thus forms a part of electronic payments. E-payment channels include those technologies that actually facilitate these payments. These include Internet-based wired channels, Bluetooth, infrared technologies, contactless payment enablers such as proximity sensors, key fobs, transponders etc., mobiles, and Personal Digital Assistants (PDAs).

The major concern relating to electronic payment is security; this entails securely transmitting payment details over the network and secure storage (Hsieh, 2001). From the point of view of the customer, apart from just security, privacy is also a huge concern. Anonymity and privacy prevent merchants from building a customer profile based on recent purchases (Wright, 2002).

Depending on the type of payment (along with the entity involved in the transaction), electronic payment transactions fall under three main categories, including retail e-payments, corporate e-payment and wholesale e-payment (Wright, 2002)

Retail e-payments includes Consumer-to-Business (C2B), Business-to-Consumer (B2C) and Peer-to-peer (P2P). Corporate e-payment includes Business-to-Business (B2B) transactions for corporate procurements, Bank-to-Business transactions, etc. Wholesale e-payment refers to payments between banks as well as payments between banks and central banks (Wright, 2002).

The figure below (Fig. 3.9) describes the scope of electronic payment transactions. This figure explains the different electronic payment transaction categories.

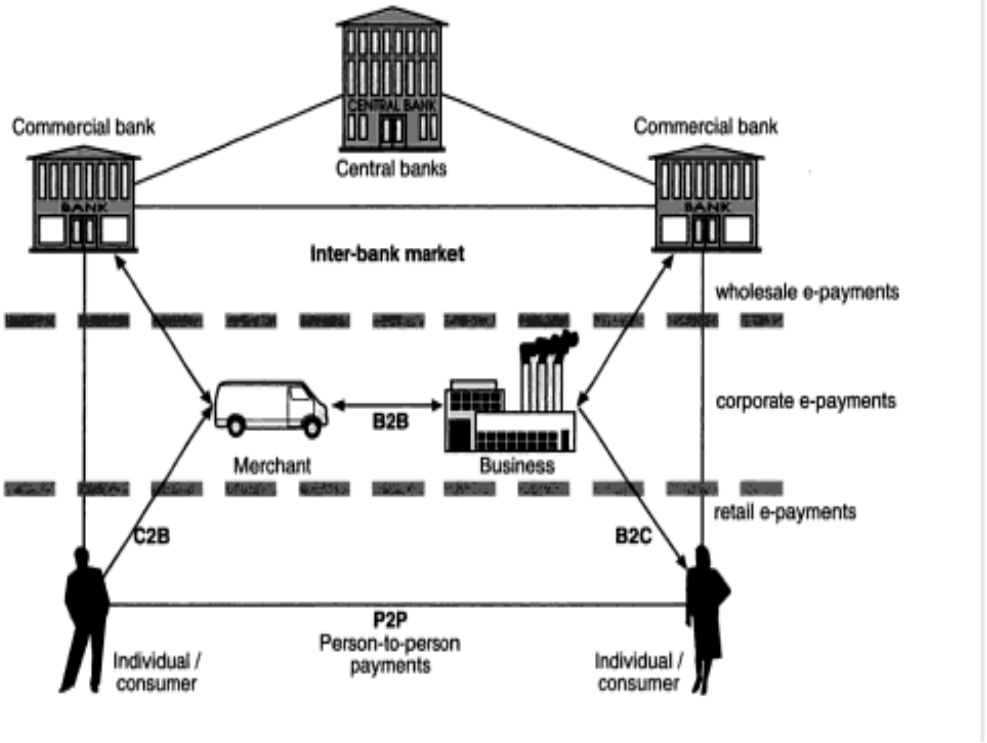


Fig 3.9: Scope of e-payment transactions

Source: Wright, 2002

There are many new technologies involved in making electronic payments secure. With the increase in the computing power and availability of technologies at lower costs, security and anonymity have become key concerns. The trend indicates that over the time, these protocols and technologies that facilitate these transactions will become insecure. There is much research

and literature available that critically analyses the existing protocols and technologies and that assesses those that contribute further by devising new technologies and/or protocols to make the electronic payments more secure and efficient. Various protocols use various security and cryptographic methodologies. For example, some use multi-application smart cards, Advanced Encryption Standard (AES), Data Encryption Standards (DES), MD5, hashing, Kerberos, Secure Hash Algorithm (SHA), Public Key Infrastructure (PKI), etc. There are various regulating authorities and standards that govern electronic payment transactions, such as the Fair Credit Billing Act (FCBA), Electronic Funds Transfer Act (EFTA) etc. Also, electronic payments are subject to more contract laws than traditional payment methods. To ensure security, the Certificate Authorities (CA) would normally be the government, banks or financial institutions. The diagram below (Figure 3.10) shows an example of electronic cheques (D O'Mahony et al., 2001):

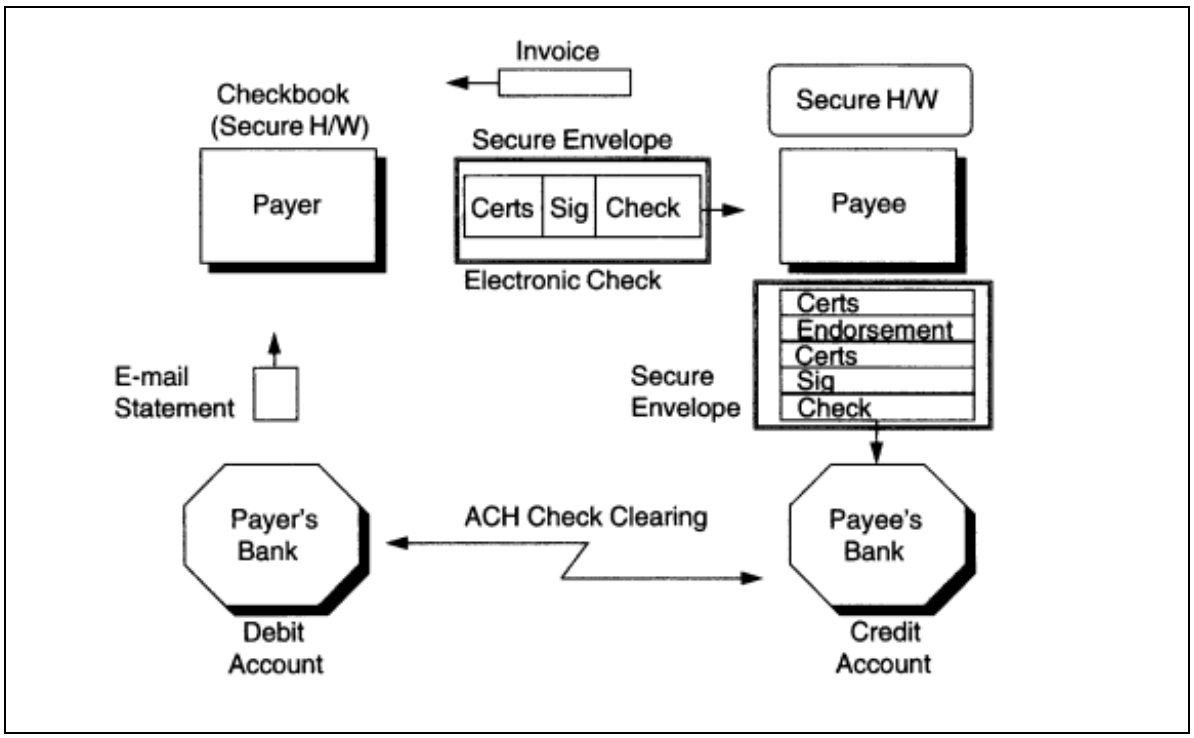


Fig. 3.10: Electronic cheques (O'Mahony et al., 2001)

One protocol by Wen et al. (2013) is based on a quantum proxy blind signature, quantum key distribution, and a one-time pad for provision of anonymity; it also provides unconditional security and supports inter-bank transactions. Some protocols focus on protecting the end-to-

end electronic payment transactions by making use of powerful client handheld devices such as key fobs, etc. Such protocols make use of a strong client-centric model, whereby the assumption is that the intermediary or the TTP is not trustworthy. This means that only the customers with the handheld device have the option to communicate with the banks or other financial institutions over the Internet (Qin, 2009). Another protocol (Raghuwanshi, 2009) makes use of an intermediary (TTP) to ensure that the electronic money that is transferred from a customer to a merchant over a telecommunications channel or network is accurate and secure. The aim of the protocol is to verify the payment order as this is critical in an arena where there is not much trust. This model makes use of the TTP, which receives messages from both transacting parties (i.e. the merchant and the customer) in order to verify the integrity of the payment. It also deals with scenarios whereby the merchant and/or the customer are dishonest.

E-commerce architecture provides payment processing service that forms the backbone of any e-commerce website. The payment processing is subject to various strict data protections rules and regulations and regulated by many parties such as the government, financial regulation bodies and authorities of the country, the central bank of the country and is subject to various laws depending on the physical location of the transacting parties. The customer and the merchant normally authenticate each other mutually in an e-commerce environment. Where there are trust issues or there are no means to be able to mutually authenticate the other a third party or an arbitrator such as the TTP, financial institution or a bank comes into play. Payment authentication is normally done using public key cryptographic mechanisms and techniques. In most cases the customer is being vouched by a bank, local building society or an financial institution that provide a platform to like an internet banking service which would enable the user to authenticate themselves and the details can be passed on by the arbitrator to the merchant who would then process the purchase order and deliver the product. One such initiative is the FAST (FSTC Financial Agent Secure Transaction); this can enable the provision of various services such as authentication of customer, payment guarantee, etc. (D O'Mahony et al., 2001).

Payment gateway is nothing but a set of servers that usually uses a secure internet channel to connect to the bank's or the financial institutions private network. This is the pivotal component in case of payment processing and this ensures that the authentication and the payment for the transactions are done not only in an effective manner but also done securely. For a gaurantee

of seamless flow of information both from the merchant and the customer and also to successfully be able to carry out the transaction payment, the payment gateway encrypts and secures the data. It is also responsible for ensuring good communication between the customer and the merchant. All these components are important as they act as a facilitator to ensure that the transactions over the internet are carried out smoothly and also in a secure way. A VPN is a virtual private network that extends a private network across the public network like internet. The main advantage of using a VPN is that it provides a secure connection even while connecting with a wireless Local Area Connection. The key components of an e-commerce portal are depicted in the diagram below (Figure 3.11) (Z Qin, 2009).

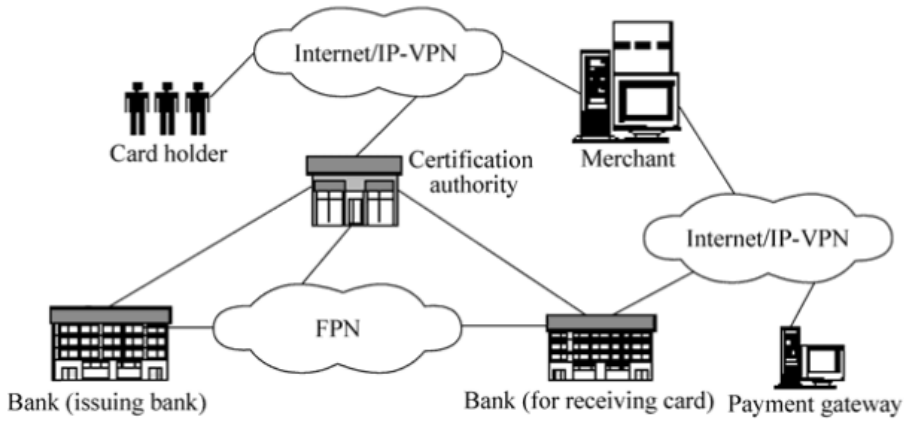


Fig. 3.11: E-commerce components (Qin, 2009)

There are three key functions that a payment gateway performs when a customer purchases goods or services online. These include:

1. Authorization whereby the customer details provided are verified
2. Clearing which helps to report the transaction and the amount to the appropriate bank ,building society or the financial institution to process the payment and
3. Reporting which helps to record and store the purchase details for the purposes of audit.

(VP Gulati & S Srivatsava, 2007).

For example, implementing a Payflow gateway requires that the appropriate PayPal APIs are are used in order for the payment to be processed. To be able to implement this, there are various SDKs that are available and these can be implemented in the code of the website that is being built. Figure 3.12 below depicts the working of a PayPal transaction (M Miller, 2011).

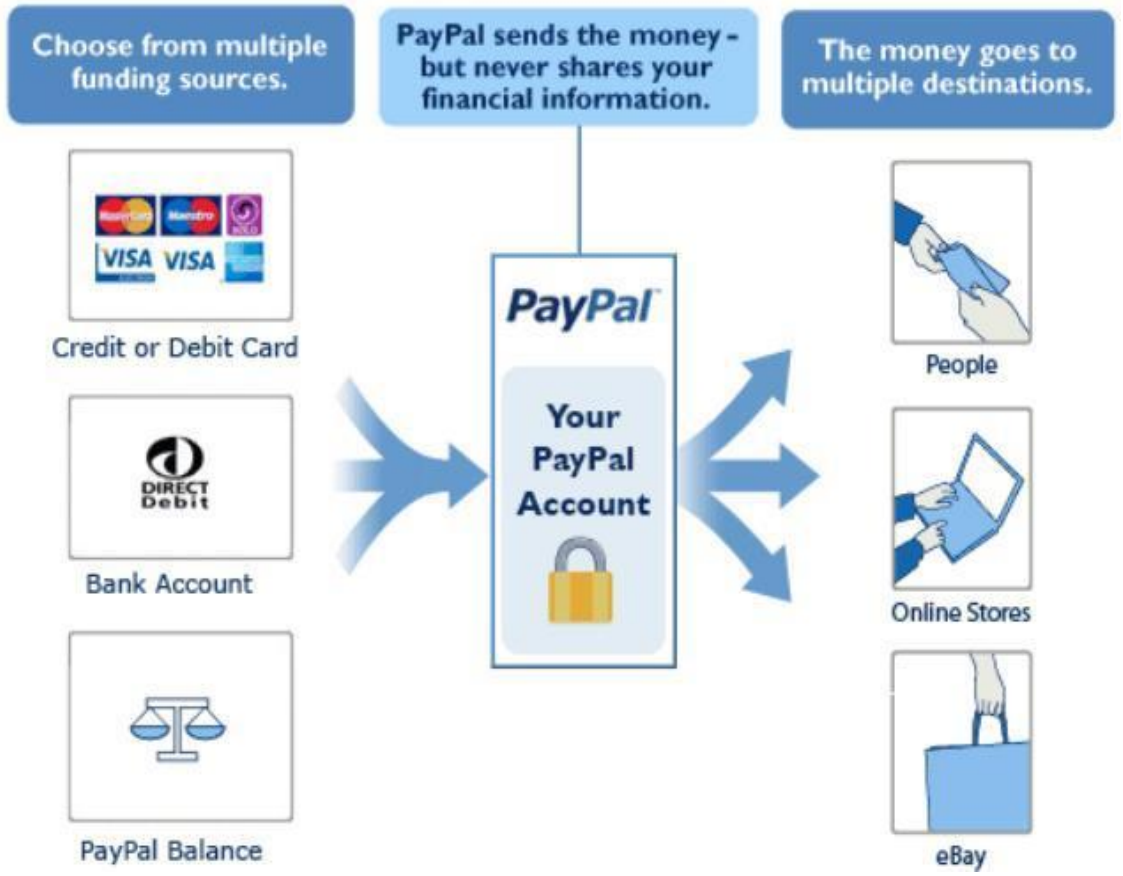


Fig. 3.12: Paypal working model (Miller, 2011)

3.8 Anonymous Electronic Cash

In an electronic payment system, electronic cash refers to the payment scheme whereby the transacting parties make use of a cash-like payment system, which is very similar to cash in the

real world. Anonymous electronic cash refers to the payment system that helps in the transfer of electronic funds from the party purchasing products or the payer (customer) to the party providing goods/services or the payee (merchant), and also helps protecting the original identity of the payer or the customer.

Anonymous electronic cash works on the cryptographic principle of blind signatures, which makes payments untraceable and hence provides anonymity and privacy to the payer. It was originally introduced by Chaum in 1983 as a means to protect the customer's identity. In Chaum's blind signature, the two key parties involved include the signer, who issues a blind signature to the payer, and the payer, who requests a signature from the signer. A blind signature satisfies two key properties, namely:

1. Blindness: this property allows a payer to request a signature on a message from the signer without having to reveal the contents of the message.
2. Unforgeability: a property which ensures that only a signer can produce valid signatures. (Chaum, 1983)

For example, Ray's protocol makes use of electronic cash in order to provide anonymity for the customer.

3.9 Dispute Resolution

A dispute can arise in a transaction when either party believes and has a reason to raise a concern that they were being cheated because the other player was being dishonest, as in traditional commerce. However lucrative and beneficial e-commerce might be, it can also suffer from disputes and conflicts. Despite the increase in the number of disputes and conflicts due to the tremendous growth of e-commerce, there is a variety of mechanisms and resources that can be employed to resolve conflicts that arise during a transaction (Tang, 2007).

In traditional commerce, disputes that arise are formally handled and settled in the courts of law. In an e-commerce scenario, however, there are other dispute resolution techniques that can be used, and these avoid the disputes being resolved in the courts. Such methods are known as Alternative Dispute Resolution (ADR), which includes mediation and arbitration (Jannadia et al, 2000).

Arbitration refers to a process whereby a neutral third party (who is unbiased) collects and collates information from both the transacting parties that are in dispute, namely the customer and the merchant. This third party then makes a decision in favour of one of the parties, and the decision made is binding on both parties (Jannadia et al, 2000).

Mediation is a process like arbitration in that it makes use of a neutral trusted third party who is unbiased. This mediator collects and collates information from both the transacting parties that are in dispute, namely the customer and the merchant. However, the mediator only facilitates both parties to come to a favourable conclusion or decision, unlike arbitration where the third party decides on behalf of both parties (Tang, 2007).

Disputes resolved online use a technique known as Online Dispute Resolution (ODR). Certain researchers (Katsh et al., 2001) describe in detail how a 'fourth party' can be used to work with and also assist the traditional trusted third party to effectively and efficiently resolve conflicts.

ODR assists in resolving disputes online and also in taking the help of the fourth party in cases relating to disputes that arise offline. It uses various opportunities that are provided by the Internet not just to employ the processes that are available but also to use the same processes to help resolve the conflict. ODR helps to mediate and arbitrate, and it allows various processes to work with neutral third parties to resolve any disputes and conflicts that arise. It is not an entirely new concept, as it has its roots in Alternative Dispute Resolution (ADR).

There is now a rapid increase in adapting to ODR for many reasons. A few of these include:

Rapid growth: there has been a tremendous and extraordinary growth in Internet technologies and in the e-commerce marketplace, resulting in a huge increase in the number of transactions.
Non-traditional marketplace growth: e-commerce has now started taking over from traditional marketplaces as well as non-traditional marketplaces.
Government agency concerns: Departments of Commerce, Federal Trade Commissions and other government agencies are now more concerned about the available dispute resolution mechanisms due to the growing number of disputes arising cross-border. (Katsh et al, 2001)

E-commerce protocols should be designed in such a way that they ensure that any disputes that might arise are reduced in number. This can be done by ensuring that both the merchant and the customer are confident of receiving their goods and/or payment. This ideally reduces the

number of messages required to resolve disputes, which in turn reduces any overheads or load on the communication channel itself, thus making the protocol efficient and effective.

3.10 Fair Exchange and Anonymity Protocols

This section aims at researching protocols that provide fair exchange and anonymity; it also discusses in detail the pros and cons of each protocol described. Each protocol is designed with a different purpose in mind and provides varying degrees of fair exchange and/or anonymity. Some provide true and strong fair exchange while others provide weak fair exchange. Similarly, some protocols provide complete anonymity, whereas some others fail to provide anonymity throughout all the e-commerce phases. This varies depending on the costs and also on the fact that true and strong fair exchange is sometimes improbable to achieve in certain scenarios and situations.

3.10.1 Frankin & Reiter

Franklin and Reiter's (Franklin & Reiter, 1997) protocol describes a method for verifying the consistency of any documents that are sent online before the exchange takes place. The protocol uses a one-way function 'f' which computes to F, such that F (x,(f(y)) = f(xy). The protocol assumes that the function f is known by both parties, and that F is known by the trusted third party. For example, consider two parties X and Y trying to exchange secret information KX and KY. It is assumed that X and Y know f(KY) and f(KX), respectively. Both X and Y send their components of the message to the TTP. The TTP compares the components to ensure that both parties are sending the correct components, and then forwards X's components to Y, and vice-versa. X and Y multiply the components received by x1 and y1 to obtain their respective messages (Franklin & Reiter, 1997).

The advantages of this protocol are:

1. The TTP does not reveal the information it receives from X or Y unless invoked.
2. The TTP can be invoked if there is a problem.

The main disadvantages of this protocol include:

1. The TTP is only semi-trusted.
2. The protocol does not work without a TTP, which leads to certain overheads.
3. The protocol also assumes that only one of the parties would be dishonest at any given time. Hence it does not cater for scenarios where more than one party is being dishonest.
4. The protocol provides only partial anonymity.

Franklin and Reiter's protocol mainly concentrates on providing fair exchange. Due to the way the protocol is designed, partial anonymity is achieved. This holds well if the protocol is not disrupted.

3.10.2 Boa's Fair Exchange Protocol

Bao's protocol (Bao, 1998) primarily makes use of an offline TTP for the provision of fair exchange. It provides fair exchange for all electronic data, including digital signatures, payment transactions and confidential data, between two transacting parties, namely A & B. The key features, which are quite unique to this protocol, are usage of offline TTP, number of messages, true fair exchange guarantee, avoiding TTP where possible and using Certificate of Encrypted Message Being a Signature Method.

It makes use of an offline TTP. This means that the TTP does not become involved with the transactions between the two parties. The TTP comes into picture only when either of the communicating parties misbehaves or for the purposes of dispute resolution. When the parties misbehave, it leads to a dispute whereby the TTP is asked to give a statement, officially known as an affidavit.

During an exchange, only three messages are sent across.

It guarantees a true fair exchange, whereby the transacting parties both receive the other's data or neither does. This avoids any loss that could be incurred irrespective of how badly either of the transacting parties behaves during the exchange process.

By providing true fair exchange, it avoids any dispute resolution where the TTP gives an affidavit relating to what happened during the transaction and attesting to the processes involved during the exchange between the parties.

It uses a cryptographic mechanism called a Certificate of Encrypted Message Being a Signature (CEMBS), which makes the protocol novel and which acts as the basis of it. This cryptographic primitive enables the signature of the parties to be encrypted on a public file without having to reveal the signature itself.

The only disadvantage from the point of view of this research is that this protocol does not provide customer anonymity. It is also important to note that this was one of the earliest protocols to guarantee a true fair exchange while making use of an offline TTP.

3.10.3 Ray's Anonymous & Failure Resilient Fair Exchange Protocol

Ray et al.'s protocol (Ray, 2005) on provision of anonymous and failure resilient fair exchange is another key protocol in the fair exchange arena. It is an optimistic protocol and invokes the Trusted Third Party only when it is absolutely necessary, that is during a transaction where either of the parties is misbehaving or when the transaction aborts unexpectedly. It uses an off-line TTP, thus avoiding any bottlenecks caused by the usage of online TTPs, which are involved in all stages of the transaction. It also avoids the vulnerabilities that are posed by TTPs, such as a DoS (Denial of Service) attack.

Ray's protocol also provides anonymity by making use of a principle first proposed by Chaum, called the blind signature, which is implemented here as electronic cash. Electronic cash transaction takes place by means of using coins of the same denomination. Therefore, to make a purchase, the customer sends multiple coins. This protocol has about nine different stages, which occur during the course of a normal transaction. The key steps that are used in the protocol are as follows:

Step1: When a customer has decided to make a purchase, he/she downloads a copy of the product which is encrypted, from the TTP.

Step 2: The customer then sends the blinded coins, which are unsigned and which are worth the total value of the product, to the bank, which then debits the amount from the customer's account.

Step 3: After the customer's account has been debited, the bank signs the blinded coins digitally and sends them to the customer. On receipt of the blind signed coins, the customer then unblinds the same to acquire the coins of the necessary value, which have been signed and authorised by the bank.

Step 4: The customer now has the coins of the necessary value. Hence he/she proceeds to encrypt the signed coins, and sends these along with the purchase order to the merchant. At the same time, the customer also creates and generates pseudo identifiers in order to keep his/her real identity a secret.

Step 5: The merchant receives the purchase order and the signed coins, and sends the encrypted product copy to the customer.

Step 6: The customer receives the product copy, decrypts it, and after verification of the product, if satisfied, sends the decryption key for the electronic coins sent earlier.

Step 7: The merchant, on receipt of the decryption keys, checks with the customer's bank to see if the coins issued are still valid.

Step 8: The bank then checks for the validity of the coins, credits the merchant's account with the appropriate amount, and then records the transaction in its database, along with the serial number of the coins that have been spent.

Step 9: The transaction is finally completed when the merchant sends the decryption key for the product to the customer.

The notation of the protocol is summarised in the table below:

Message	Notation
Message 1: The customer downloads copy of encrypted product	TP =>C : [m; K_M]
Message 2: Customer sends blinded coins	C=>M: PO, [CC(PO), C_{prv}], [[PT, K_0><K_{c2}], B_{prv}],B
Message 3: Bank signs blinded coins digitally and sends to customer	$\mathrm{M} \Rightarrow \mathrm{C}$: $[[\mathrm{CC}(\mathrm{PO}), \mathrm{C_{prv}}], \mathrm{M_{prv}}], [mr, K_{\mathrm{M}} \times K_{\mathrm{M_1}}$ $[r, K_{\mathrm{M_1}}], [\mathrm{CC}([r, K_{\mathrm{M_1}}]), \mathrm{M_{prv}}],$ $[\mathrm{CC}([mr, K_{\mathrm{M}} \times K_{\mathrm{M_1}}]), \mathrm{M_{prv}}]$ **OR** $\mathrm{M} \Rightarrow \mathrm{C}$: Abort

Message 4: Customer encrypts the coins and sends these with the purchase order to the merchant and generates pseudo identifiers for keeping his/her identity secret. Sends decryption key to the merchant on receipt of the encrypted product and the decryption key	$C \Rightarrow M: \ [K_{C_2}^{-1}, M_{pub}], [CC([m, K_M \times K_{M_1}]), C_{prv}]$ **OR** $C \Rightarrow M: \ \text{Abort}, [CC([m, K_M \times K_{M_1}]), C_{prv}]$
Message 5: Merchant receives the decryption key, checks with the Customer Bank to check for validity and transaction is complete when the product decryption key is sent	$M \Rightarrow C: \ [K_{M_1}^{-1}, C_{pub}], [r^{-1}, C_{pub}]$

Table 3.1: Notational representation of Ray's Anonymous and Failure Resilient Fair Exchange Protocol

The trusted third party here acts as a mediator to establish whether both the parties, namely the customer and the merchant, are acting fairly. If there is any unfairness, the TTP requests more details, as the protocol is based on the offline TTP model. Anonymity is achieved here as the customer does not give out his/her details to the merchant, and also makes use of the blind signature concept.

The verification of this protocol by Kong et al. (2004) reveals that the TTP is only semi-trusted, and has the capability to alter messages or to masquerade and become an intruder. This is one of the drawbacks of the protocol.

The following diagram (Fig. 3.13) shows the key steps involved in the protocol's execution.

Symbol	Interpretation
C, M, and TP	Customer, Merchant, and Third Party
CB and MB	Customer's Bank and Merchant's Bank
C_{acct}	Customer's bank account with CB
M_{acct}	Merchant's bank account with MB
m	Product the customer is purchasing
PO	Purchase order used to order product m
T_i	Transaction involving purchase of m
A_{prv}, A_{pub}	A's private and public keys
A_{iprv}, A_{ipub}	A's private and public keys used only in T_i
B_{cprv}, B_{cpub}	Common private and public keys for banks
$A \Longrightarrow B : X$	A sends X to B
$[X,K]$	Encryption of X with key K
$CC(X)$	Cryptographic checksum of X
K_1	Key given to the TP by M
K_1^{-1}	Decrypting key of K_1 held by third party
K_2	Key that is compatible with K_1
K_2^{-1}	Decrypting key corresponding to K_2
r	Random number chosen by merchant for T_i
r^{-1}	Multiplicative inverse of r modulo N_2
$\mathcal{P}$	Payment token used for paying for product

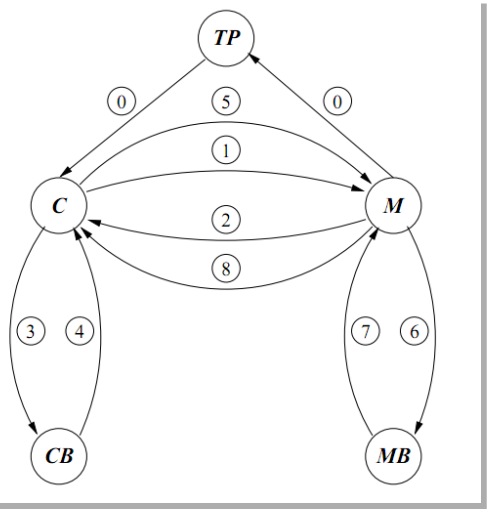


Fig 3.13: Execution steps of Ray's protocol (Ray, 2005)

This protocol implements fair exchange and dispute resolution mechanisms that are automatically performed within the scope of the protocol. However, it does not provide a true fair exchange. It distributes the function of the TTP across many TTPs, thus increasing the robustness of the protocol. It adopts a payment mechanism (called electronic cash) that enables provision of anonymity. The other drawbacks include:

1. Usage of asymmetric cryptography for encryption/decryption. This is not very efficient or effective if the content is huge.
2. It uses electronic cash based on the principle of Chaum's electronic cash. This method has its vulnerabilities; for example, Chaum's concept assumes that the bank cannot break the signature that is used by the party paying cash. The scheme has an unfortunate property in that the bank can frame Alice (the one paying cash) as a multiple spender. This in turn makes void any legal significance. To prevent the frame-up, it is assumed that Alice has a digital signature scheme and a certified copy of her public key. Because digital signatures are being used here, Alice is protected against a frame-up, only computationally and not unconditionally, which represents vulnerability (D Chaum et al., 1990).

3. For purposes of anonymity, customers create pseudo identifiers with a one-time private key and a public key for their transactions. This becomes a bottleneck in cases where customers try to generate multiple identities for many different transactions.

3.10.4 Zhang's Anonymous Purchase and Physical Delivery Protocol

The next protocol that is key is the practical fair exchange protocol for anonymous purchase and physical delivery, proposed by Zhang et al. (2006). This protocol is effective and efficient, and provides the means to support fair document exchange over the Internet for e-commerce transactions. It incorporates an RSA-based cryptographic mechanism, which provides a measure to recover the party's decryption key offline. The idea is based on the principle that the recovery of the offline key is dependent on the verifiable and recoverable decryption key. This verifiability property allows the other party to check the correctness of the key without having any knowledge whatsoever of the original key. The recoverability property allows the parties to decrypt the encrypted key to obtain the original key. However, this process necessitates the good management of keys and the secure transmission of those keys.

3.10.5 Zhang's Anonymous and Fair Exchange Protocol

Another protocol by Zhang et al. (2003) on anonymity and fair exchange describes the exchange of information between two transacting parties, namely P_a and P_b, with the assistance of an off-line TTP P_t. The methodology for the process of generating and verifying P_b's commitment (CO_b) assures P_a that P_t can re-cover r_b from co_b, which then allows P_a computation of P_b's key. In this scenario, P_a is unable to obtain r_b after handing over all the information to P_b. Also, the key recovery conducted by P_t does not require any information about the identities, locations, exchanged documents and keys of P_a and P_b, so the impact of P_t's security on the protocol is weakened. This, coupled with anonymous communications between the parties involved, demonstrates the protocol's true anonymity.

It is important to note that Zhang's protocol provides both anonymity and fair exchange, and this uses symmetric key cryptography and an off-line TTP that is not involved entirely in the transactions. The protocol assumes that both the transacting parties have a document and a symmetric key to encrypt or decrypt the document. The first stage before the protocol is invoked is to get the documents certified by the relevant authorities. For example, a digital signature is certified by a CA, a payment token is certified by a bank, etc. This certification

process is key as it allows each of the transacting parties to verify the correctness of the documents and the decryption key, and it ensures fair exchange in the transactions.

Anonymity is a key feature of this protocol and this is achieved by making use of communication channels that are anonymous; it also makes use of anonymous electronic cash. This protocol has two sub-protocols, namely document exchange and key recovery.

The following table summarises the key stages of the first protocol which is the document exchange protocol

Message	Meaning
P_a ($^{E}k_a(D_a)$,kr_a) => P_b	A party represented by P_a (anonymous) first initiates the transaction by sending in his or her encrypted document to the other transacting party P_b. The encrypted document, $^{E}k_a(D_a)$ along with the item sent kr_a is used to compute the key, which is done in step number three.
P_b($^{E}k_b(D_b)$,kr_b, CO_b)=> P_a	After receiving the document from P_a, the other party (P_b) sends his or her encrypted document, represented by $^{E}k_b(D_b)$, along with the item sent (kr_b) for the computation of the key, which is done in step number four. This is along with P_b's commitment (CO_b), which is produced in relation to the symmetric keys (kr_a and kr_b). This is done if P_b successfully verifies the document received, $^{E}k_a(D_a)$. The commitment CO_b assures P_a that P_t, which is the TTP, would definitely be able to help P_a recover the key k_b from co_b without actually

	knowing the key k_b, and also be able to
$P_a(r_a)=>P_b$	The next step involves P_a sending an item r_a to P_b after verifying $^{E}k_b(D)_b$ and the commitment CO_b. P_b now uses the item r_a to compute k_a from the kr_a.
$P_b(r_b)=>P_a$	Similar to the previous step, the next step involves P_b sending an item r_b to P_a after verifying $^{E}k_a(D)_a$ and the commitment CO_a. P_a now uses the item r_b to compute k_b from the kr_b.

Table 3.2: Zhang's Document Exchange Protocol notation

The second sub-protocol describes the offline key recovery process and consists of two key stages, where each of the parties invoke the TTP P_t to help recover r_b from Co_b to compute k_b from the kr_b, and then r_b from Co_a to compute k_a from the kr_a, respectively. The second stage involves P_t sending the recovered r_a and r_b to P_b and P_a, respectively, to enable them compute the symmetric keys.

The drawback however in this protocol is the number of messages exchanged, which makes it very complex. The protocol also does not provide mechanisms for fair exchange throughout the e-commerce transaction, i.e. there is no provision for fair exchange during the negotiation phase, and this protocol does not address the issue of what would happen if either party withdraws the purchase. Another drawback is the heavy reliance on the TTP, which provides the security of the transactions. Thirdly, though the protocol claims to offer anonymity, the customer is required to disclose his/her public key during the transaction. If the customer uses the same public key again for different transactions, the merchant can collect details such as customer preferences.

3.10.6 Zhang's Mutual Authentication Protocol

Another protocol by Zhang et al. (2006) provides both anonymity and fair exchange. In addition to these, the protocol also provides a feature whereby the correct item could be ensured before the transaction. It makes use of a 'commit buffer' account which temporarily holds the customer's credit details until they are passed on to the bank. It consists of six different phases and has a total of 11 messages.

This makes the protocol quite cumbersome. One more disadvantage of the protocol is that it assumes that the commit buffer being held by the TTP would always be sufficient to hold enough data. It does not discuss what would happen if there is an error in the commit buffer or if a buffer overflow occurs. This protocol has not been formally verified or model-checked to evaluate efficiency and correctness.

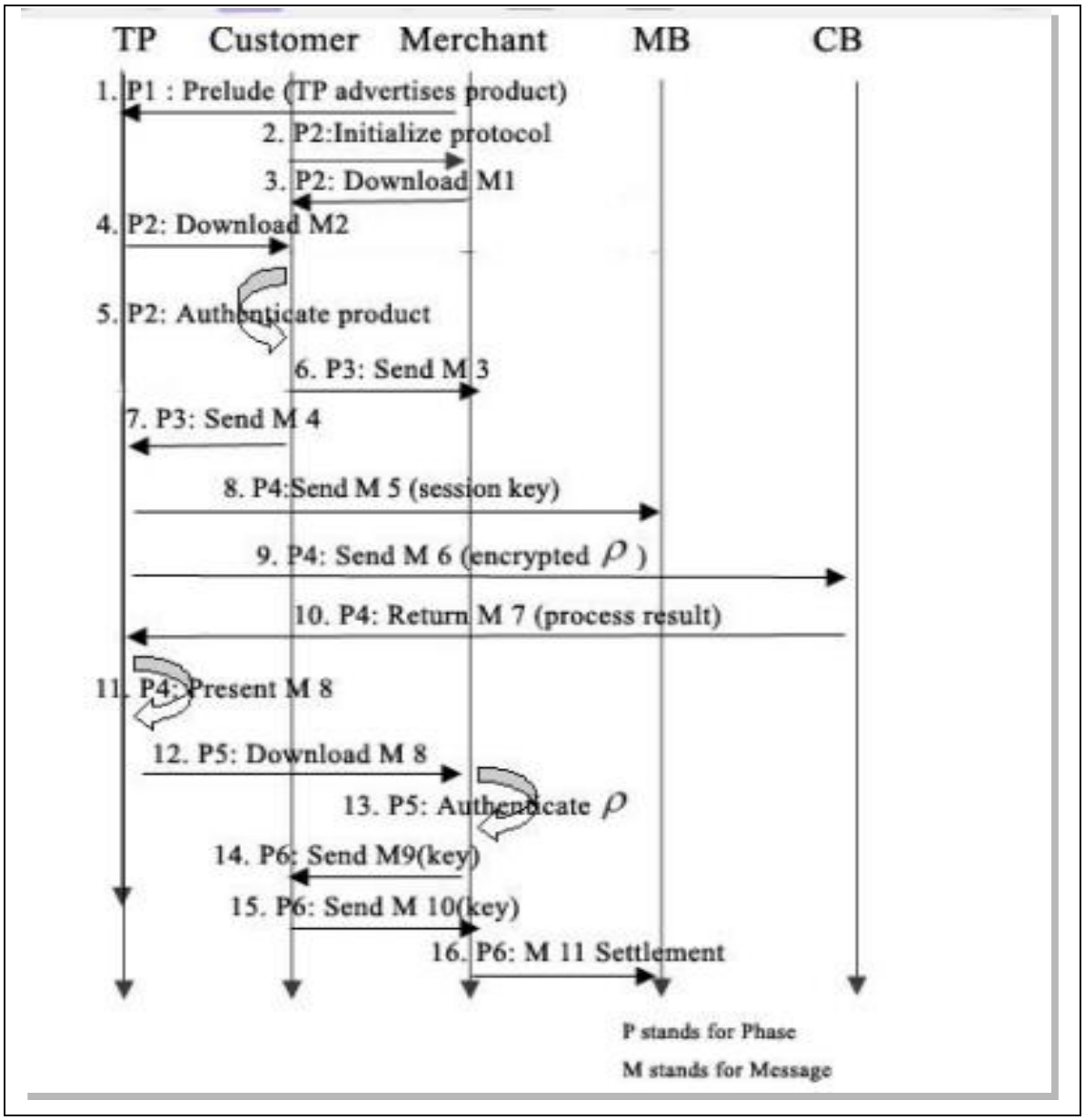


Fig. 3.14: Execution of Zhang's Mutual Authentication protocol (Zhang, 2006)

3.10.7 Zhang's Non-Repudiation Protocol

Another protocol by Zhang (1996) provides fair exchange by making use of an online TTP. The main aim of the protocol however is provision of non-repudiation of receipt, that is, the receiver cannot deny having received the message/product or cash. This protocol mainly aims at providing non-repudiation and does not provide anonymity for either of the transacting parties.

3.10.8 Wang's Protocol

Based on an RSA cryptographic mechanism of key exchange, Wang's protocol (2005) mainly concentrates on the contract signing phase in e-commerce. It primarily deals with RSA-based signatures and addresses fairness and abuse-free mechanisms. This protocol discusses fair exchange in terms of signature exchange, and does not concentrate on providing anonymity.

Though there are various protocols that provide anonymity or fair exchange in general, only three protocols (Ray, 2005; Zhang, 2006; Zhang, 2003) provide both of these features. It is therefore imperative that the scope of this research is narrowed down to only these three protocols.

3.11 Research Gaps

From the above literature, it can be clearly seen that there are only three protocols (Ray, 2005; Zhang, 2006; Zhang, 2003) that provide anonymity and fairness during e-commerce transactions. However, there are various weaknesses and gaps in these three protocols. The key gaps are as follows:

1. Ray's protocol (2005) uses a TTP as an arbitrator for transactions, however the TTP is only semi-trusted thus is able to alter messages or become an intruder

2. Ray's protocol (2005) requires that customers create pseudo-identifiers for their transactions which becomes a bottleneck.

3. Zhang's protocol (2006) has too many messages (11 messages across 6 different phases) which makes it very cumbersome.

4. Zhang's protocol (2006) also assumes that a commit buffer is held by the TTP and does not take into consideration what would happen if the buffer is unavailable.

5. Zhang's protocol (2003) does not provide fair exchange throughout all the phases of the e-commerce transaction.

6. Zhang's protocol (2003) does not provide complete anonymity as it requires the customers to disclose his/her public key during the transaction which might lead to the merchant collecting details such as customer preferences.

The six gaps mentioned above in the literature are overcome by the current protocol. The novelty of the protocol lies in the fact that it provides anonymity and fairness like the other protocols (Ray, 2005; Zhang, 2006; Zhang, 2003) and also ensures that it overcomes those gaps/drawbacks mentioned above thus ensuring that the protocol is robust and efficient.

3.12 Summary

This chapter has discussed e-commerce in detail; it has addressed the advantages, disadvantages and restrictions of e-commerce, fair exchange, types of fair exchange protocols (along with a detailed analysis of different fair exchange protocols, highlighting the pros and cons of each), anonymity, electronic cash and the means to achieve anonymity. It discussed the issue of trust and how trust plays a key role in e-commerce transactions. It also described how this trust can be established in e-commerce. It detailed payment gateway systems and described how transactions and payments are processed as well as emphasising the importance of security. It discussed the legal and regulatory aspects of e-commerce, dispute resolution mechanisms, and the role of Trusted Third Parties. It identified gaps in the literature, justifying the need for a new and more efficient protocol.

CHAPTER 4: CONCEPTS AND ASSUMPTIONS

The aim of this chapter is to give a broad overview and to detail key definitions for the various cryptographic concepts and mechanisms that form the basis of the proposed protocol. It includes all the key assumptions that the proposed protocol is based upon. The idea of this chapter is to enable the reader to familiarise himself/herself with the main ideas, techniques and methods that are being used.

Chapter Objectives:

- Introduce the reader to the various key terminologies, concepts and cryptographic mechanisms that are being used throughout the research.
- Understand various technologies, algorithms and other cryptographic principles and primitives.
- Explain the key assumptions based on which the proposed protocol is designed and developed.

4 Concept and Assumptions

The aim of this chapter is to present all the cryptographic concepts that are to be used in the proposed protocol and also to present the key assumptions made in the protocol.

Though this research is not on cryptographic methods, cryptography plays a key role in the security and provision of anonymity and fair exchange. Hence, it is essential for the reader to understand the underlying concepts and this chapter thus provides a background into the key concepts that are being used in the protocol. It discusses in detail the different types of cryptography and proceeds to explain RSA, hashing and Certificate Authority, and then discusses the assumptions upon which the proposed protocol is based.

4.1 Types of Cryptography

Cryptography is the science of locking up information (usually on a personal computer) so that only authorized people can access it (Kirkby, 2001). There are two different types of cryptography: these are Symmetric Key Cryptography and Public Key Cryptography (commonly known as Public Key Infrastructure or PKI).

4.1.1 Symmetric Key Cryptography

Symmetric Key Cryptography as described by the author (Kirkby, 2001) refers, in the simplest terms, to making use of the same key for both encryption and decryption; the key that is used in the process is referred to as a Symmetric Key. The key that is used here for encryption and decryption needs to be distributed prior to the communication over a secure channel or medium.

Encryption is defined as, *"The process of changing plaintext into ciphertext using a cryptographic algorithm and key."* Ciphertext refers to the text in encrypted form (Kirkby, 2001).

Decryption is defined as, *"The process of changing ciphertext into plaintext using a cryptographic algorithm and a key"* (E Barker et al., 2012).

A key in cryptography refers to a secret (similar to a password) that is used to encrypt and decrypt messages (G Wooledge, 2011).

The National Institute of Standards and Technology (NIST) defines key as, "*A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Examples of cryptographic operations requiring the use of cryptographic keys include: The transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, the computation of a digital signature from data, the verification of a digital signature, the computation of an authentication code from data, the verification of an authentication code from data and a received authentication code, the computation of a shared secret that is used to derive keying material and the derivation of additional keying material from a key-derivation key (i.e., a pre-shared key).*" (E Barker, 2012)

As described by GC Kessler (2013), in this type of cryptography, the key is known both to the sender and the receiver; that, in fact, is the secret. The author also discusses the biggest difficulty with this approach, which is the distribution of the key. There are two categories of secret-key cryptography schemes; these could either be stream ciphers or block ciphers. Stream ciphers are those ciphers that operate on a single bit (byte or computer word) at a time, and that implement some form of feedback mechanism so that the key is constantly changing. A block cipher is a form of cipher whereby one block of data is encrypted at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher, whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

4.1.2 Public Key Cryptography

Public Key Cryptography (PKI), as defined by G Wooledge (2011), refers to cryptography where one key is used to encrypt, and a matching key is used to decrypt. These two keys together are called a key pair. One of these keys is called the secret key or private key, and should be kept secure. The other is called the public key and should be given out to everybody who would want to participate in the communication or transaction (G Wooledge, 2011).

Another author (Schneier, 1996) describes how the concept of Public Key Cryptography is based on the mathematical principle that the two keys (the private and the public key) are related. There are various cryptographic encryption techniques that make use of Public Key Cryptography. The most commonly used are the Diffie-Hellman algorithm, ElGamal and RSA. In a

public key encryption, the sender encrypts the message using the pubic key, and the receiver of the message decrypts the message using the private key.

Modern Public Key Cryptography as a concept was first described by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. It is based on the mathematical concept of one-way functions, whereby it is easy to compute but inversing is nearly impossible (GC Kessler, 2013). Public key cryptography is depicted in the image below (Figure 4.15)

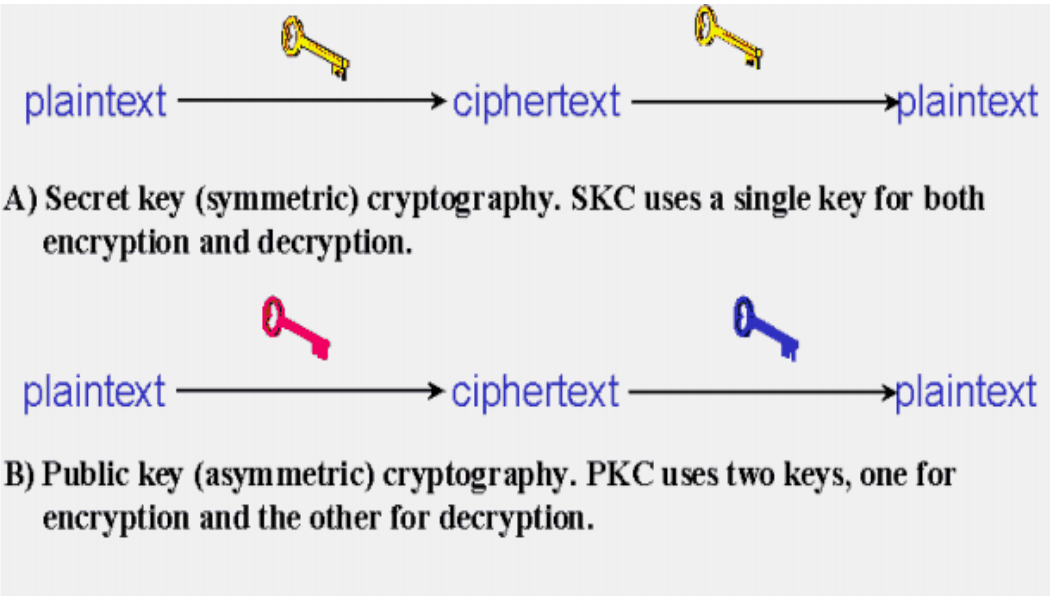


Figure 4.15: Different types of cryptography (Figure source: GC Kessler, 2013)

4.1.2.1 RSA

RSA is a public key cryptography system that is named after the three mathematicians who developed it, namely Ronald Rivest, Adi Shamir and Leonard Adleman. It is one of the most popular PKI encryption systems being used today. It is used for various purposes, namely key exchange, digital signatures or encrypting small blocks of texts, and is used in over hundreds of software products. The public key is known to anybody and the private key is only known to the party that owns it. It uses variable-sized encryption blocks and the size of the encryption key is also variable. RSA works as mentioned below:

A large number *n*, which is a product of two prime numbers *p* and *q*, is generated. *n = p*q*, where both *p* and *q* are prime. The next step is to calculate Ø (*n*). This is done using the formula *Ø(n) = (p-1)*(q-1).* The third step is to select an integer *e* whereby the following condition is satisfied: *1<e<* Ø(*n*) and e is relatively prime to Ø(*n*). The fourth step of the RSA algorithm calculates *d* using the formula $d = e^{-1} \bmod Ø(n)$. Now all the variables are calculated.

The next steps determine the private key and the public key for the RSA algorithm.

1. The public key is (*e,n*).
2. The private key is (*d,n*).

Now that the keys are generated, the message to be encrypted (M) is taken and the size of the message is determined. If the size of M is greater than *n* (which is the product of two primes *p* and *q*), then the message is broken down into smaller blocks, where each block is less than *n*.

Encryption is done using the following:

$C = M^e \pmod n$

To decrypt the message or the block, the following is used:

$M = C^d \pmod n$

(Rivest, Shamir & Adleman, 1978)

RSA is believed to be highly secure as the key-pair is derived from a very large number *n*, which is a product of two large prime numbers *p* and *q*. As a rule, these prime numbers have 100 or more digits and therefore the product of these would yield twice as many digits as the prime factors. The public key contains *n* but it is very difficult for the attacker to compute the prime factors *p* and *q*. Hence, the private key remains safe and becomes almost impossible to obtain just from *n*. The success of RSA is based on this fact that it is virtually impossible to compute the factors and is hence secure. Given the ability of computers to process the factors of large numbers, the attacker is now able to find out the prime factors of numbers with more than 200 digits. However, it is still difficult to find out the prime factors of two large numbers that have the same size; it takes a while to compute the prime factors as there is currently no known factorization algorithm that can compute the factors within a reasonable amount of time. Time

is a critical factor here, as most messages need to be secure only for a reasonably short period of time, for example, during message transit (GC Kessler, 2013).

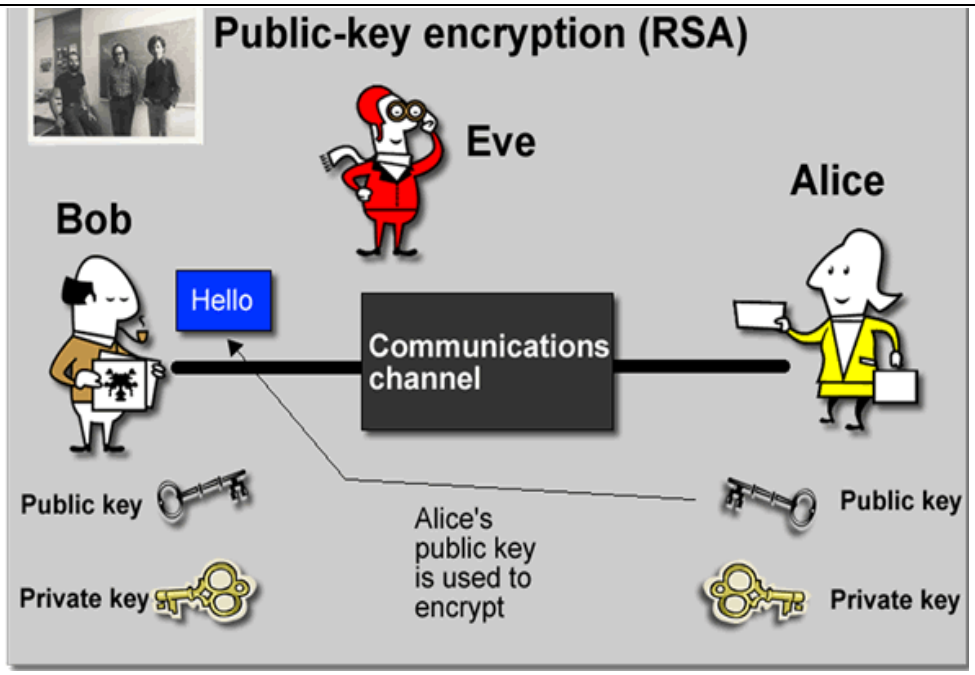


Figure 4.16: RSA public key encryption

Figure Source: RSA Encryption and Decryption (Bill's Design, 2013)

4.2. Hashing

Hash functions use the mathematical concept of irreversibility to encrypt a message. It takes a variable length input and delivers a fixed length output, which makes it mathematically impossible to determine the plaintext from the ciphertext (or even the length of the plaintext). Hash functions, also called message digests and one-way encryption, are algorithms that, in cryptographic terms, do not use a key. The main uses of hash include the provision of digital fingerprinting for a file's contents or for a message (to ensure that the message or the file has not been modified). Most operating systems and certain web-based systems make use of a hash

to encrypt passwords, storing the hash in the database rather than the password itself; this helps achieve integrity.

Many different hash algorithms are being widely used today. Some of the most common algorithms are message digest, MD2, MD4 and MD5.

Message Digest: commonly referred to as MD. This algorithm provides a hash output of 128 bit length from any arbitrary length of plaintext message.
MD2: this is mainly used in systems that have very limited capacity in terms of memory, such as smart cards.
MD4: very similar to MD2, this was developed by Rivest, one of the developers of the RSA algorithm. This is specifically used in fast processing software solutions and technologies that are time critical.
MD5: again, developed by Rivest, this was originally designed to ensure that the weaknesses of MD4 were resolved. Much slower than MD4.
Secure Hash Algorithm (SHA): this produces a hash output of 160 bits. It is an algorithm for NIST's Secure Hash Standard (SHS). (G Wooledge, 2011)

4.3 Certificate Authority

In simple terms, a Certificate Authority (CA) can be defined as a server or a trusted organisation whose main responsibility is to issue and maintain certificates. A certificate in cryptography refers to a mechanism that binds or puts together the public key and all other related components in order to uniquely identify the identity of the person who claims to be the owner. In an e-commerce environment, the parties do not trust each other. A CA thus helps to verify the identity of a person or organisation and issues a certificate to that effect. A CA does this by binding the public key to the individual's identity. This in turn implies that the CA takes the liability for the individual's identity.

A Certificate Authority (CA) in short is thus responsible for creating, handling and revoking certificates (where necessary). When a certificate is revoked by the CA, it is securely stored in a Certificate Revocation List (CRL), which is updated periodically. The standard for the CA to create

and issue certificates is described by X.509, which describes the different components or fields and the acceptable values for each field (S Harris, 2010).

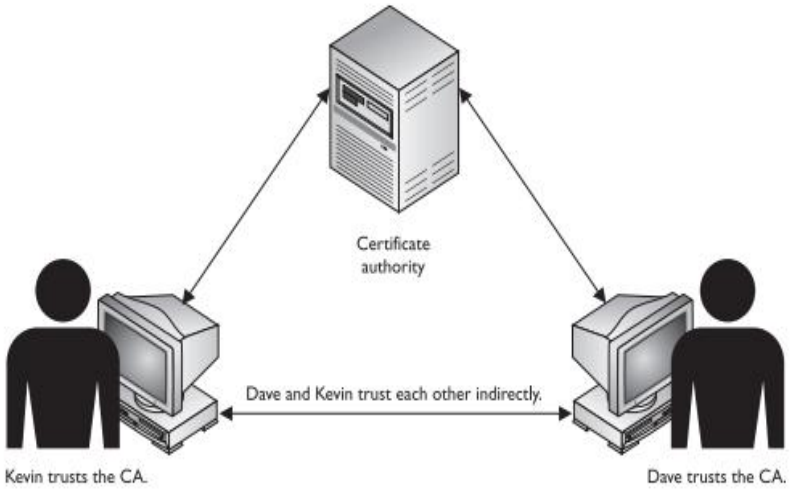


Figure 4.17: Establishing trust between two parties by a Certificate Authority (CA)

Figure Source: S Harris, 2010

4.4 Digital Signatures

In a traditional commerce environment, where two parties meet face-to-face, an offer and acceptance can be proved when both parties physically sign a contract. However, in an e-commerce world, where the parties do not see each other, a digital signature is used.

A digital signature is obtained by combining a user signing a hash value with the private key; this assists in the provision of authentication, integrity and non-repudiation. Digital signatures are used to replace passwords in many systems that require a stronger form of authentication. Many algorithms are used for digitally signing documents or messages. The most commonly used algorithms are RSA, El Gamal and DSA.

A digital signature can be defined as, *"An electronic signature based upon the cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified."* The act of encrypting this hash value with a private key is called digitally signing a message (S Harris, 2010).

Digital signatures are created in accordance with the Digital Signature Standards (DSS) issued by the National Institute of Standards and Technology (NIST). NIST describes the uses of digital signatures as follows: *Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.*(NIST, 2013)

To encrypt a message, the sender uses the private key and the receiver uses the public key to verify the identity of the sender, as only the sender will have the private key.

4.5 Notations and Participants - Proposed Protocol

This section of the document aims at describing the key participants or entities in the proposed e-commerce protocol and how these participants are denoted. It also gives a brief description of the role each participant plays in the proposed e-commerce protocol.

1. Merchant: Merchants are entities (individual or corporate) that have digital products to sell. This entity has the authorisation to advertise its intention to sell such goods online from the producer of the online products. Merchants, in return for sale of the digital products, take cash (in the form of electronic cash) from the customer, which is then redeemed at the Merchant's bank. In the protocol, Merchant is represented by the letter M.
2. Customer: Customers are entities (individual or corporate) that require digital products sold by the merchant. Customers verify the authenticity of the products using a TTP and purchase the online product in exchange for electronic cash that is withdrawn from the Bank. Where the transaction has not been carried out as required, the Customer can initiate arbitration process. In the protocol, Customer is represented by the letter C.

3. Bank: Banks help withdrawal and redemption of electronic cash to the Merchant and Customer. The Bank is also responsible for verifying details when requested by the TTP. In the protocol, Bank is represented by the letter B.
4. Trusted Third Party: Refers to an individual or corporate that helps in mediating the e-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. The Producer gives permission to the Merchants to sell these products online to customers. In the protocol, Producer is represented by the letter P.

4.5.1 Protocol Assumptions

The proposed e-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 e-commerce transaction; hence it does not deal with Transport Layer Security. Secondly, the protocol does not dictate who the Trusted Third Party should be; it assumes that the Customer and Merchant have mutually agreed on who the TTP would be, and hence, is not 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. Therefore, TTP is used heavily in the initial stages while trust is being established. This assumption acts as a building block to develop a protocol that will break through this weakness of the nature of the TTP.
2. The TTP cannot read or modify messages sent.
3. The TTP will not collude with any other party.
4. All parties involved in the protocol will behave rationally.

5. The protocol avoids any replay attacks by making use of a cryptographic mechanism, such as a digital signature and time-stamped messages. Time stamps can also be used in cases of dispute resolution.
6. The protocol also assumes that a resilient connection is present between all parties involved, namely, the Customer, Merchant and the TTP. This means that all messages sent are relayed appropriately to the appropriate recipients.
7. With regard to payment, the protocol makes use of digital cash and any double payments 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.

4.6 Summary

This chapter has given the reader an overview of the key terms, assumptions and cryptographic principles and mechanisms that are to be used in the proposed protocol. This chapter has thus acted as a prelude to the 'proposed protocol' chapter in so far as the reader has gained an idea about the various methods and algorithms that are being used and is now also aware of how each cryptographic primitive is used to achieve certain specific security goals.

CHAPTER 5: IMPOSING ANONYMITY AND FAIRNESS PROTOCOL

This is the key chapter of the research. The aim of this chapter is to introduce the reader to the proposed protocol, namely, 'Imposing anonymity and fairness'. It provides a brief about the actual research problem, the central research question and the gaps in the current research environment as well as the need for designing a new protocol. It then discusses the protocol steps in detail, categorising each step into a specific e-commerce phase. It clearly describes how this protocol helps overcome the current gaps in research and literature. Additionally, it performs a scenario analysis that is used to prove that the protocol is effective. This is achieved by taking into account the various possible scenarios and determining how the protocol works, as well as assessing whether the protocol achieves its aims in each of the scenario specified.

Chapter Objectives:

- Introduce the reader to the proposed protocol and describe the steps of the protocol in detail.
- Understand how various steps of the protocol could be classified under different e-commerce phases.
- Understand the performance of the protocol and check that it satisfies all the conditions and achieves the key properties, namely, anonymity and fair exchange, in all instances.

5 Imposing Fairness and Anonymity Protocol

The primary aim of this chapter is to discuss the underlying mechanisms of the protocol and to detail the techniques used in the protocol. It also aims at analysing and discussing in detail the actual protocol.

The chapter begins with the approach the protocol takes and the underlying evolutionary concept of the protocol, followed by a detailed explanation of the Imposing Fairness & Anonymity (IFA) protocol through a discussion and analysis to check that the protocol satisfies the criteria of fair exchange and anonymity.

5.1 Research Problem and Requirements

The main objective of this research is to propose an efficient and effective protocol for e-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.'s anonymous and failure resilient fair-exchange e-commerce protocol, Zhang's Mutual Authentication Protocol and Zhang et al.'s Efficient Protocol for Anonymous and Fair Exchange. Although these protocols have achieved both the above-mentioned characteristics of anonymity and fair exchange, inherent problems related to these protocols remain, as discussed in earlier chapters. The protocol also makes use of an online Trusted Third Party (TTP) to mediate between the transacting parties and for any dispute resolution purposes. In addition, it is aimed at providing fair exchange throughout all phases of an e-commerce transaction. The proposed protocol has the following success criteria:

1. Fair Exchange: The key goal is to ensure true fair exchange where either both the parties or none of the parties receives the goods at the end of the transaction. This ensures that honest parties are not being punished for the deeds of the dishonest party.
2. Anonymity: Using the blind signature concept, the protocol ensures that the customers' identities are kept secret, thus providing privacy. This is achieved by using the concept of blind cash (Chaum, 1990).

3. Trusted Third Party (TTP): The protocol ensures that the TTP which is partially trusted or semi-trusted does not have the ability to masquerade as another party or to alter or read messages in any way.
4. Single Payment Token: The efficiency of the protocol is increased as the payment is made by using a single token rather than multiple tokens with the same denomination.
5. Simplicity: The protocol makes use of symmetric key cryptography wherever possible, for example, encryption and decryption of messages to ensure that it is simple; it also reduces any computational bottlenecks and key management overheads.

5.2 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, which describe the messages sent between all parties involved in the protocol process.

Step 1: The Merchant obtains approval to sell the digital contents from the Producer (P), who owns the digital copyrights for the product.

Step 2: The Merchant, on receiving acknowledgement from the Producer to sell the products, proceeds to obtain verification of the digital contents through the Certificate Authority (CA). The CA verifies the identity of the merchant and issues a certificate that is digitally signed. The certificate issued by the Certificate Authority is of the standard X.509 format.

Step 3: The Merchant uploads the product details online to his website to attract potential customers. Along with the product details, the merchant also uploads the certificate received by the CA to help enhance the perception of trust.

Step 4: The interested Customer now views the product and verifies the digital signature to ensure 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 and encrypted 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, avoiding any file tampering.

Step 8: The 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 TTP with the hashed, time-stamped and encrypted digital product. The product is encrypted to avoid any misuse by intruders or the TTP and is hashed to be able to be verified if tampered with.

Step 10: The TTP now verifies this and sends the same to the Customer.

Step 11: Merchant and the Customer now directly send each other the hash to verify.

Step 12: Each party verifies the hash individually and exchanges private keys.

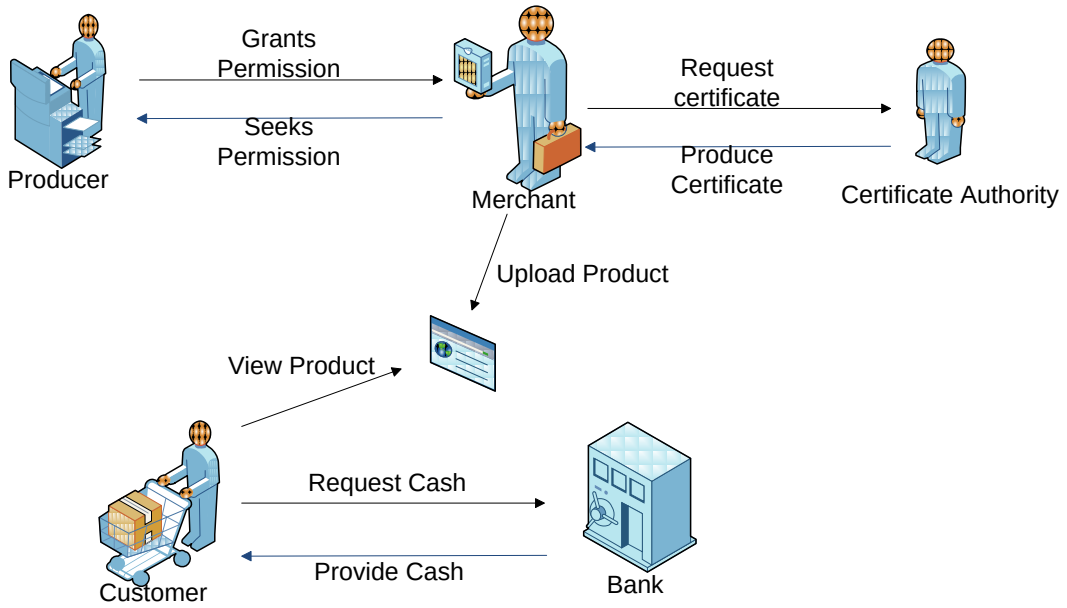
Step 13: The Merchant requests the TTP to send the electronic cash that the customer sent previously.

Step 14: The TTP sends the encrypted cash to the Merchant who then decrypts the same using the key exchanged in Step 12.

Step 15: The Customer requests the TTP to send the digital product sent by the Merchant.

Step 16: The TTP sends the encrypted product to the customer who then decrypts it using the keys exchanged in Step 12.

Step 17: The Merchant sends a request to the bank to redeem the cash.



Key:

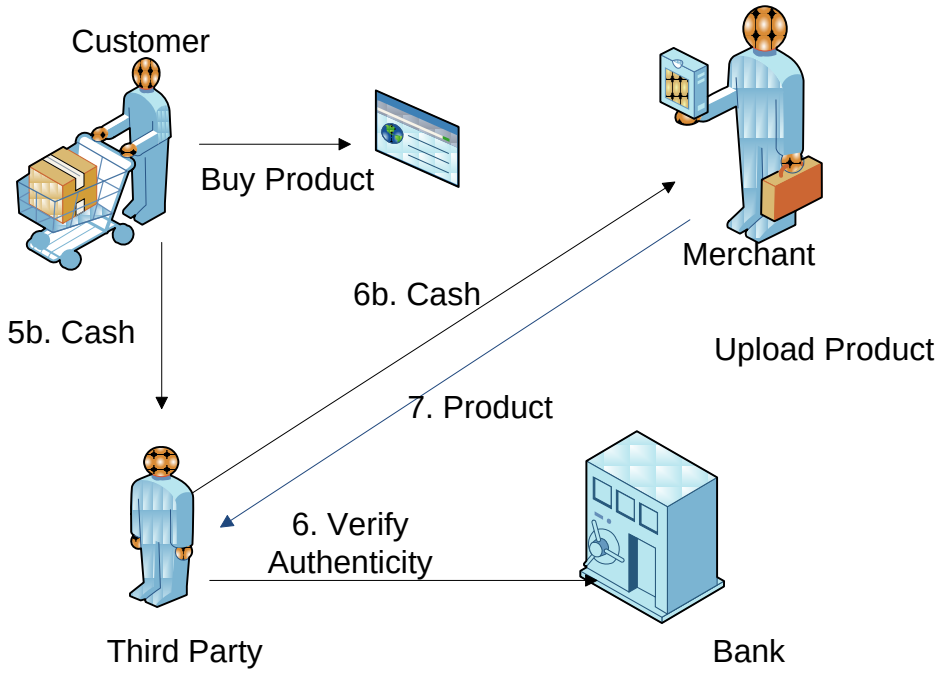
1. The Merchant (M), obtains permission to sell the digital contents from the Producer (P).

2 The Merchant contacts the Certificate Authority (CA) to obtain a certificate for the electronic identity. The Merchant then uploads the product details online for potential customers to browse and buy.

3. The Customer withdraws cash (electronic cash) from the Bank.

4. The Bank (B) issues the requested cash to the customer.

5. The Customer uses the Merchant's website to browse products of interest.

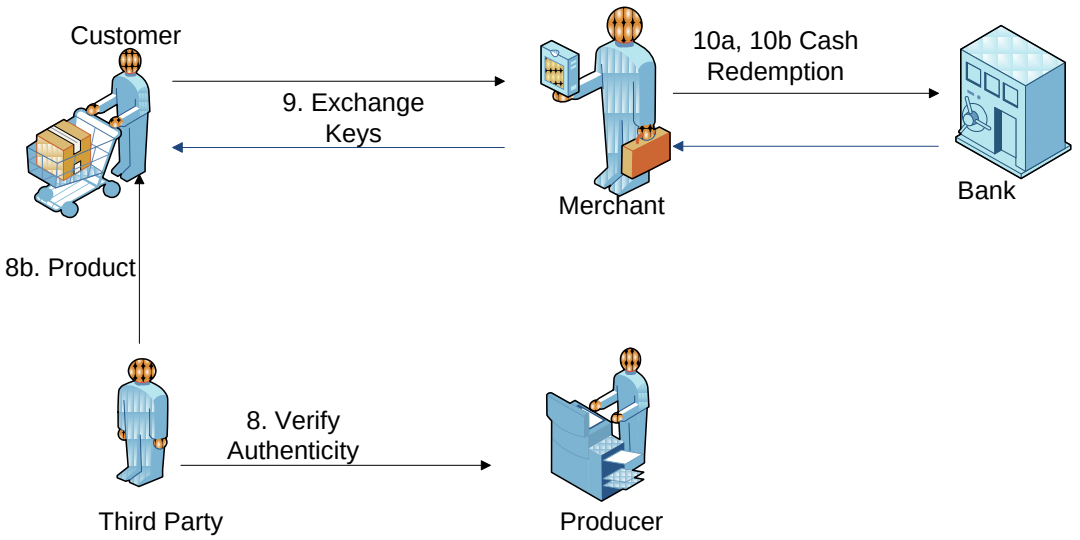


5b. When the decision to purchase is made, the Customer contacts the Trusted Third Party (TTP) with a hashed, time-stamped and encrypted electronic cash transfer.

6a. The TTP verifies the hash of the encrypted cash with Customer's bank.

6b. Once verified, the TTP indicates the Customer's interest to the Merchant and sends the encrypted electronic cash.

7. The Merchant replies to the TTP with a hashed, time-stamped and encrypted digital product.



(Steps 11 -17 of the protocol)

8a. The TTP verifies the hash of the encrypted digital product with the Producer (P).

8b.Once verified, the TTP sends the encrypted digital product to the Customer.

9. The Merchant and the Customer exchange the hash value for the digital product/electronic cash for verification and the decryption information (key).

10a. Once the transaction is completed, the Merchant sends a request to the Bank to redeem the electronic cash from the Customer.

10b. The Bank credits the Merchant's account with the cash.

Fig 5.18: Imposing Fairness Protocol

5.2.1 Protocol Stages

The steps described above gives a gist of the proposed protocol. This section is aimed at providing a detailed analysis of the individual stages of the e-commerce transaction.

The protocol covers five different stages of the standard e-commerce phases; these are:

1. Pre-Negotiation Phase
2. Negotiation Phase
3. Withdrawal Phase
4. Purchase Phase
5. Arbitration Phase

5.2.1.1 Pre-negotiation phase

This phase of the e-commerce transaction, as discussed in previous chapters, is the first phase in any e-commerce transaction. This phase deals specifically with gathering data, identifying needs of customers, identifying key suppliers, determining the trustworthiness of the suppliers etc.

In the proposed protocol, the first three steps form the pre-negotiation phase. In these steps, the Merchant identifies the potential supplier, acquires permission to sell the digital product online, and obtains a digital certificate from the Certificate Authority to improve the perception of trust in the potential customers.

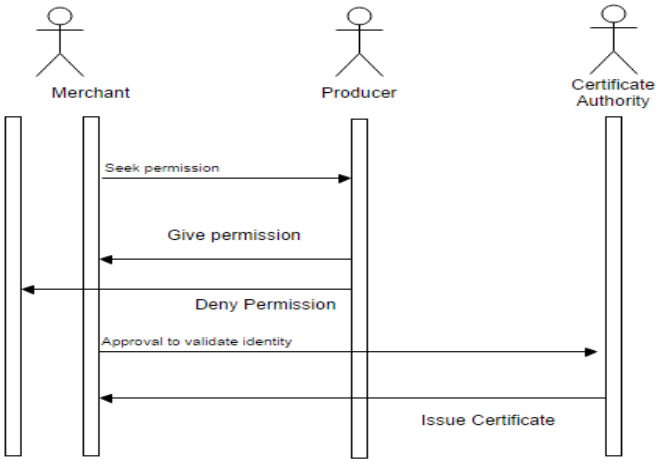


Fig 5.19: Pre-Negotiation Phase of Imposing fairness protocol

5.2.1.2 Negotiation phase

During this phase, the actual formal relationship is being established. The potential customer views the product, along with any attached terms and conditions and attempts to understand the legality of the contract. This phase is when the customer shows interest in buying the product and negotiations happen between the merchant and the customer.

In the proposed protocol, steps 3 and 4 falls under the category of negotiation phase. This is where the merchant shows interest in selling the digital products by uploading the products to the online website and where the customer views the product of interest and can also verify the merchant's digital certificate with the Certificate Authority (CA). Any questions that the customer has regarding the product are also answered in this stage.

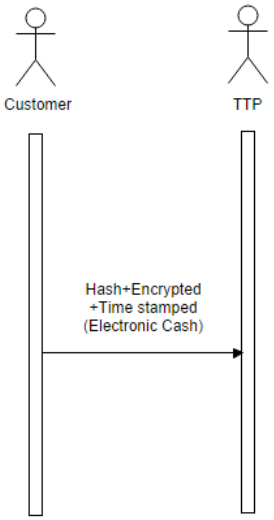


Fig 5.20: Negotiating phase of the Imposing Fairness Protocol

5.2.1.3 Withdrawal phase

This phase of the e-commerce transaction describes areas which concern withdrawal of cash for the purposes of purchasing electronic products from the merchant. It is a phase where the customer requests his/her bank to issue electronic cash and where the banker then checks the

customer's account to ensure that he/she has sufficient funds in the account. Once the banker is certain of the funds in the account, electronic cash is then issued to the customer. Steps 5 and 6 of the proposed protocol deal with the withdrawal phase.

The customer has now identified the digital product of interest and has verified the costs with the merchant. The customer has also reviewed the Terms and Conditions attached to the contract and is also satisfied with the trustworthiness of the merchant. The customer now wants to make a purchase and requires cash. Therefore, the customer requests the bank to withdraw electronic cash and the bank approves the request, based on the satisfactory funds available in the account of the customer.

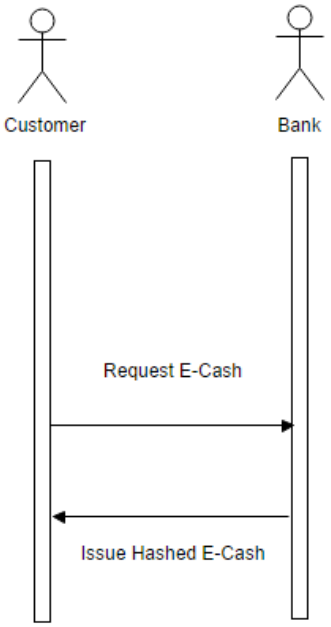


Fig 5.21: Withdrawal phase of the Imposing Fairness Protocol

5.2.1.4 Purchase phase & Arbitration phase

This phase of the e-commerce transaction describes the actual purchase of electronic goods. This is where the offer made is accepted. Acceptance shows the willingness of both the transacting parties to deliver the product and pay the money as stated in the contract. If for any

reason, either of the parties is not satisfied, the contract could be re-negotiated or the parties are free to withdraw.

The arbitration phase involves interference from a trusted, unbiased party (TTP in the case of this protocol) to resolve any issues relating to distrust or issues that might occur when either of the transacting parties behave in an untrustworthy manner. Dispute resolution could also be involved.

This protocol has an overlapping purchase and arbitration phase, as it involves the TTP entirely once the customer has decided to make the purchase. Hence, from the 7th step onwards, the protocol covers the purchase and arbitration phases; thus, the arbitration phase arises every time the TTP is involved and the actual purchase phase occurs when the electronic cash is delivered to the merchant and the digital product is delivered to the customer.

After the digital product and electronic cash are delivered to the appropriate parties, disputes may still arise. In such cases, records from the TTP can be used to effectively resolve the issues. This protocol, however, does not describe the process to be used for dispute resolution.

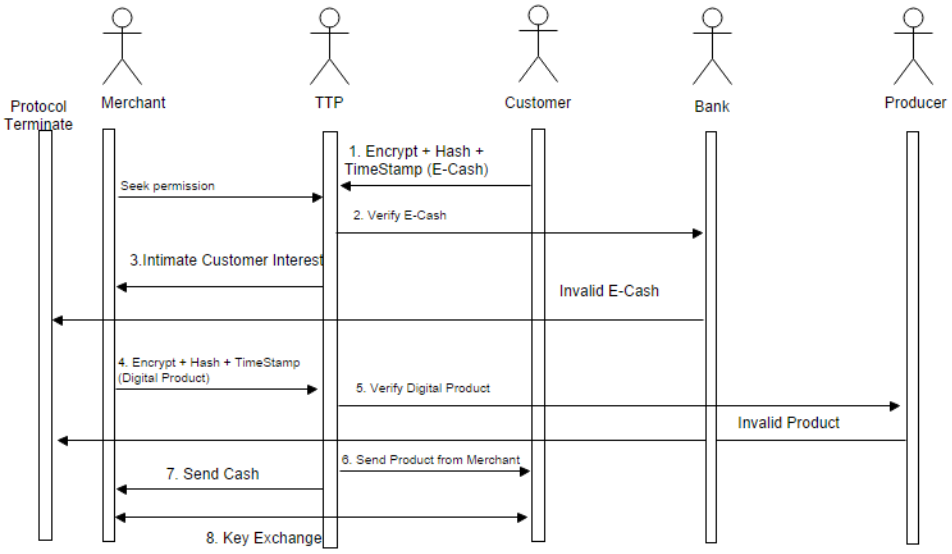


Fig. 5.22: Purchasing and arbitrating phase of the Imposing Fairness Protocol

5.3 Protocol Analysis

The aim of this section is to analyse the proposed protocol in order to be able to identify any flaws in the protocol and 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 assesses whether or not the proposed protocol is able to overcome the drawbacks mentioned in the other protocols discussed earlier. It also identifies areas where disputes may arise and how the protocol enables the transacting parties to resolve these conflicts.

In addition, this section details the effectiveness and efficiency of the proposed protocol through comparison with other protocols, and concludes with a detailed analysis of dishonesty detection in this protocol.

5.3.1 Fair Exchange

One of the desirable key 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 as is the Certificate Authority (CA). The Trusted Third Party (TTP) is semi-trusted as it is capable of masquerading. The other two parties, namely, the Customer (C) and the Merchant (M) are very much capable of misbehaving and being dishonest. This section shows a case-by-case scenario of all the possible actions that are considered dishonest. The following scenarios give a more detailed analysis that help identify dishonesty amongst the participants.

Scenario 1: The Merchant sends a different price to the Customer. 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 sends a different product to the Customer. This inconsistency is again easily detected by the Customer when he/she checks the hash of the message.

Scenario 3: The Merchant 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.

Scenario 4: The Customer sends no cash. This is identified as the decryption key for the digital product sent by the Merchant would not be exchanged with the customer to enable decryption of the message and usage of the product.

Scenario 5: The Customer sends wrong amount. This inconsistency is identified by the Merchant when he checks with the Bank to verify the funds of the Customer.

Scenario 6: The Trusted Third Party (TTP) modifies the message sent by the Merchant. This is easily identified by the Customer as the hash of the message would not match.

Scenario 7: The TTP modifies the message sent by the Customer. This is easily identified by the Merchant as the hash of the message would not match.

Scenario 8: The TTP does not forward the digital product to the Customer or the electronic cash to the Merchant. This is rendered useless as the Customer and the Merchant (M) exchange the decryption keys in private without the involvement of the TTP. Without the key, the TTP 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. 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 TTP but before receiving the electronic cash, decides not to proceed with the transaction. This again is easily managed as the Merchant can refrain from exchanging the decryption key with the Customer. Without the decryption key, the Customer cannot access or make use of the digital product.

5.3.2 Anonymity

Another of the protocol's key features is the 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 and the Trusted Third Party (TTP) are not aware of the true identity of the Customer, as the Customer does not share this.

In the next phase (the withdrawal phase), only the Bank (B) is aware of the Customer's 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 the real identity of the Customer 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 TTP is aware of the Customer's identity, as the Customer does not share any of his/her personal details. Furthermore, since anonymous electronic cash is used for the transaction, it is impossible to trace the Customer's true identity.

In the arbitration phase again, the Customer does not share any details regarding his/her 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, other than the Customer him/herself 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 e-commerce transaction; thus, the proposed protocol provides complete anonymity to the Customer.

5.3.3 Payment Security

One of the other key features that the protocol assures is security of payment. As in traditional commerce, a threat also exists to the security of payments in e-commerce. However, unlike in traditional commerce, payment security has additional challenges that are very different.

Key researchers in the area of payment security have identified two key challenges (Xue et al., 2005; D Chaum, 1983; Lin et al., 2006). These key factors are:

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

This section of the document aims at highlighting various scenarios where the transacting parties attempt to either double-spend the electronic cash or forge electronic cash, describing in detail what happens when such attempts are made.

Scenario 1: The Customer tries to forge the electronic cash to gain illegal benefits from the Bank.

Argument: 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 attempts to forge other values of electronic cash, the Bank would be able to easily identify the anomaly.

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

Argument: 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 Bank's private key, the Merchant would never be able to gain access to this. Hence, any attempt made by the Merchant to forge the value of the electronic cash would be easily identified by the Bank.

Scenario 3: The Customer 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.

Argument: This again is not possible. Every time the Customer spends electronic cash, the Bank enters the details of the spent cash in its database. Thus, when the Customer sends electronic cash, the Bank decrypts the message and compares the kept cash with the spent cash; therefore, if the sent message is already stored in the spent cash database, the Bank can easily identify the anomaly.

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

5.3.4 Dispute Resolution

After the completion of an e-commerce transaction, as in a traditional commerce transaction, there might be disputes that require resolution. Unlike in traditional commerce, however, the disputes are varied in nature and the handling of disputes and their resolution is quite different in an e-commerce scenario.

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

1. Customer received the correct digital products that he/she ordered
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 specifications
4. Customer did not receive the product at all

The protocol aims at achieving the first output, 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, there are three key outcomes that are the most likely to occur. These outcomes are as follows:

1. The Merchant received the correct payment for the digital product(s) sold.
2. The Merchant received an incorrect payment for the digital product(s) sold.
3. The Merchant did not receive the payment for the digital product(s) sold.

Again, the protocol aims at achieving the first outcome, as that is the most desired. 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 e-commerce transaction and describes 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 (C)	Merchant (M)	Honest?	Outcome
Receives the correct product	Receives the correct payment	Merchant: √ Customer: √	No Dispute
Receives the correct product	Receives incorrect payment	Merchant:√ Customer: X	Dispute raised by the Merchant
Receives the correct product	Does not receive the payment	Merchant: √ Customer: X	Dispute raised by the Merchant
Receives incorrect product	Receives correct payment	Merchant: X Customer: √	Dispute raised by the Customer
Receives incorrect product	Receives incorrect payment	Merchant: X Customer: X	Dispute raised either by the Customer or the Merchant
Receives incorrect product	Does not receive the payment	Merchant: X Customer: X	Dispute raised either by the Customer or the Merchant
Receives correct product but defective	Receives correct payment	Merchant: X Customer: √	Dispute raised by the Customer
Receives correct product but defective	Receives incorrect payment	Merchant: X Customer: X	Dispute raised either by the Customer or the Merchant
Receives correct product but defective	Does not receive the payment	Merchant: X Customer: X	Dispute raised either by the Customer or the Merchant

Table 5.3: Dispute Scenario based on product and payment

From the above table(Table 5.3) it can be seen that there are twelve possibilities where a dispute might arise. It can be noted that if both the parties (the Customer and the Merchant) receive the end products, then there is no cause for dispute.

Similarly, during the e-commerce transaction, there are various possibilities where disputes might occur. The following sub-chapter identifies the possibilities where the transacting parties might be dishonest and describes the scenarios that might lead to a dispute.

5.3.5 Detection of Dishonesty

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

1. Sending an incorrect payment
2. Making a payment that is encrypted with a different key than the one exchanged with the Merchant
3. Using an invalid signature on the payment

When the Merchant receives the payment details from the TTP, he/she will check the signature on the payment along with the encryption key. If the encryption key is different to the one that is being exchanged, the Customer's dishonesty is clearly identified.

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
3. Using an invalid signature on the product

Similarly, when the Customer receives the product details from the TTP, he/she 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 identified.

In worst case scenarios, there is also a possibility that the TTP acts as an intruder and masquerades. The TTP 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 TTP, the hash value of the message changes and hence the Customer or the Merchant can easily detect the interception, as the messages are time-stamped, and hence, it is easy to check the time when the message was originally sent;

therefore, either party can easily detect any dishonesty in the Trusted Third Party and reject the messages if the time frame has elapsed. The TTP can sometimes act dishonestly by not sending the products or the cash to the appropriate, designated party. In this case, it will not be of any use, as the Merchant and the Customer alone have 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 or the Merchant does not send the product/cash, the protocol automatically terminates as these are sent to the TTP, which only sends the cash to the Merchant and product to the Customer on receipt of both items. Hence, the TTP will not be disadvantaged by having sent the product and/or cash.

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

1. Merchant sends the correct product and the correct encryption key. This is the perfect situation and proves that the Merchant is honest.
2. Merchant sends the correct digital product but the wrong decryption key. This implies that the Merchant is dishonest.
3. Merchant sends the incorrect digital product (faulty or 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.

Table 5.4 below explains the possibilities for the Merchant.

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

Table 5.4: Possibilities for Merchant's Dishonesty with reference to Digital Product and Decryption Key

With reference to the encryption key and cash, there are again four different possibilities that exist for the Customer with specific reference to electronic cash and hash value. These are:

1. Customer sends the correct cash and the right encryption key. This is the perfect situation and proves that the Customer is honest.
2. Customer sends the correct electronic cash but the wrong decryption key. This implies that the Customer 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. Customer sends the wrong electronic cash and the correct decryption key, which indicates that the Customer is dishonest.

Table 5.5 below explains the possibilities for the Customer.

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

Table 5.5: Possibilities for Customers' dishonesty with reference to Electronic Cash and Decryption Key

The four possibilities for the Merchant with reference to the product and the digital signature are:

1. Merchant sends the correct product and the right digital signature. This is the perfect situation and proves that the Merchant is honest.
2. Merchant sends the correct digital product but the wrong digital signature. This implies that the Merchant is dishonest.
3. Merchant sends the incorrect digital product (faulty or wrong product) and 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.

Table 5.6 below explains the possibilities for the Merchant (M).

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

Table 5.6: Possibilities for Merchant's dishonesty with reference to Digital Signature and Product

Similarly, the four possibilities for the Customer with reference to the product and the digital signature are:

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

Table 5.7 below explains the possibilities for the Customer.

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

Table 5.7: Possibilities for Customer's dishonesty with reference to Electronic cash and Digital Signature

5.3.6 Scenario Analysis

This section aims at performing a scenario analysis. Various scenarios 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 Table 5.8 below.

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

Table 5.8: Outcome based on behaviour of Customer and Merchant

To discuss in detail, the first scenario is where the Customer and the Merchant are both being honest. In this scenario, the first stage is where the Customer and Merchant are both being honest and send the correct electronic cash and digital product, respectively, to the Trusted Third Party (TTP). In the second step, the Customer and Merchant now exchange the keys and in the third step, they are able to use the key to decrypt the digital product and electronic cash, respectively. When both the parties are being honest, they exchange the keys and then receive their respective products from the TTP. This is the key step in the protocol.

This is depicted in Figure 5.23 below.

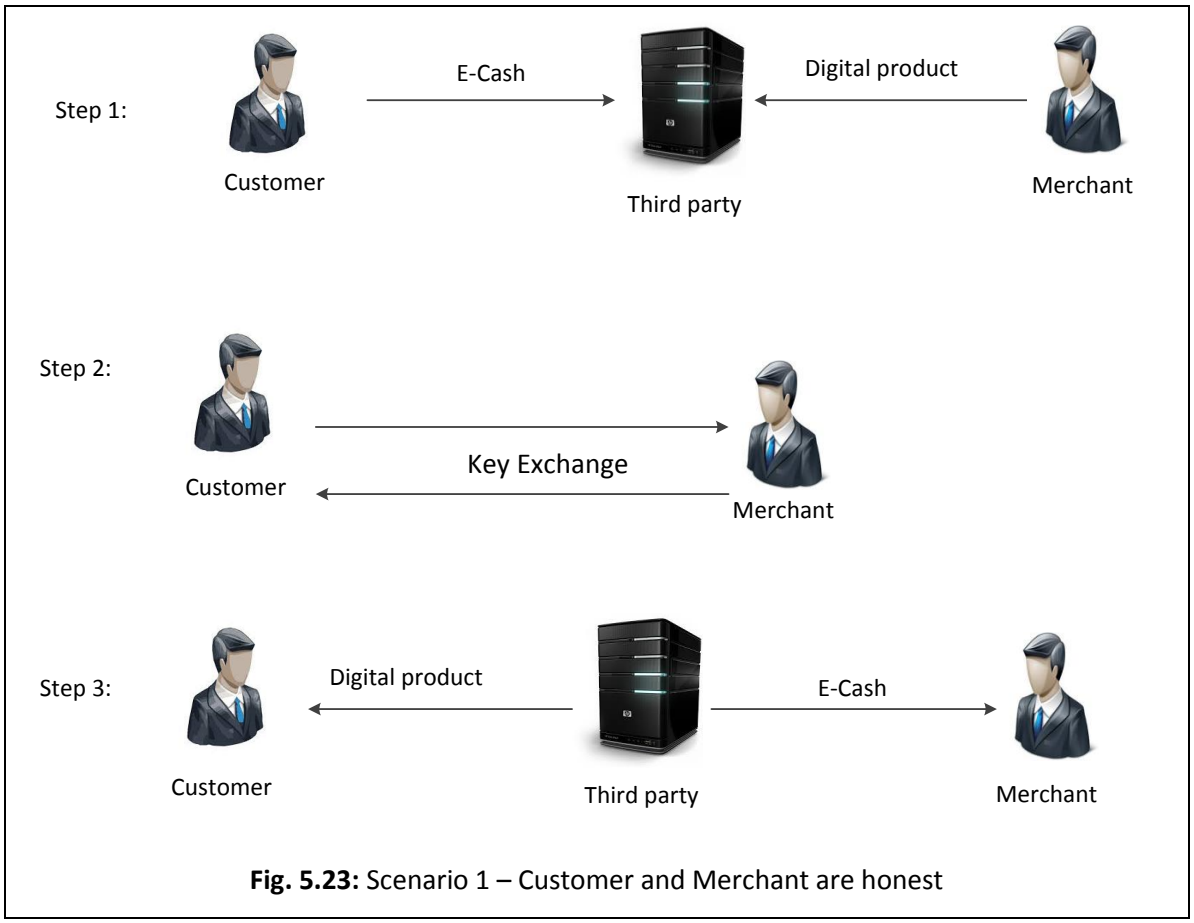


Fig. 5.23: Scenario 1 – Customer and Merchant are honest

Scenario 2: Customer is honest and the Merchant is dishonest

In this scenario, it is assumed that the customer is being honest by sending the electronic cash to the Trusted Third Party but the Merchant is being dishonest by not sending the digital product. In this case, steps 2 and 3 from the above scenario do not take place. The key exchange happens only on confirmation from the TTP that it has received the cash and the product. Since this does not happen, in this case, the Customer can understand that the Merchant is not trustworthy. Hence the Customer would not exchange the key with the Merchant. Hence, unlike in Figure 5.23, there would only be one step in this scenario, as depicted in Figure 5.24 below.

Fig. 5.24: Scenario 2 – Customer honest, Merchant dishonest

Since there is no communication from the Merchant, the protocol cannot proceed as it identifies that the Merchant is being dishonest. Hence, the communication stops. Although the electronic cash is sent by the Customer, it is of no use to the TTP as there is no decryption key that has been exchanged. The TTP, hence, cannot misuse the electronic cash.

Scenario 3: In this scenario, the Customer is being dishonest by not sending the electronic cash and the Merchant is being honest by sending the digital product to the TTP. Similar to the above scenario, steps 2 and 3 of the first scenario do not take place. This is because the key exchange can only happen if the TTP actually sends a confirmation to the parties after receiving the items from both parties. This is clearly depicted in Figure 5.25 below.

Since there is a lack of communication from the point of the Customer, the protocol stops further exchange process as it identifies that one of the transacting parties, the Customer in this case is not being honest. The Merchant need not be worried about the digital product being misused by the TTP, as the product is encrypted and the Trusted Third Party does not have the decryption key to be able to decrypt the product and use it.

Fig. 5.25: Scenario 3 – Customer Dishonest, Merchant Honest

Scenario 4: In this scenario, both the Customer and the Merchant are being dishonest. They do not send the electronic cash or the digital product respectively and try to gain undue advantage by assuming the other party would be honest. In this case, nothing happens as the TTP does not receive the electronic cash from the Customer or the digital product from the Merchant. This is clearly depicted in Figure 5.26 below.

Fig. 5.26: Scenario 4 – Customer Dishonest, Merchant Dishonest

Since there is no communication from both the Merchant and the Customer, after a timeout period, the protocol stops as it is assumed that neither party is interested or that both parties are behaving in a dishonest manner. This just leads to the abrupt termination of the protocol.

We have now analysed what happens when either party is dishonest. The next step is to analyse what happens when either party wishes to withdraw. Here, we are assuming that the first step of sending the electronic cash or the digital product to the TTP has already occurred and the Customer or Merchant at this stage wishes to withdraw. The following table, Table 5.9, describes all the scenarios relating to this:

Customer	Merchant	Result
Sends the electronic cash to the TTP and wants to continue	Sends the electronic cash to the TTP but wants to withdraw	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

Table 5.9: Withdrawal scenarios for Customer and Merchant

Scenario 1: Both parties send items to the TTP and both the parties wish to continue the transaction normally. The steps that follow this are clearly shown in the diagram below, Figure 5.27).

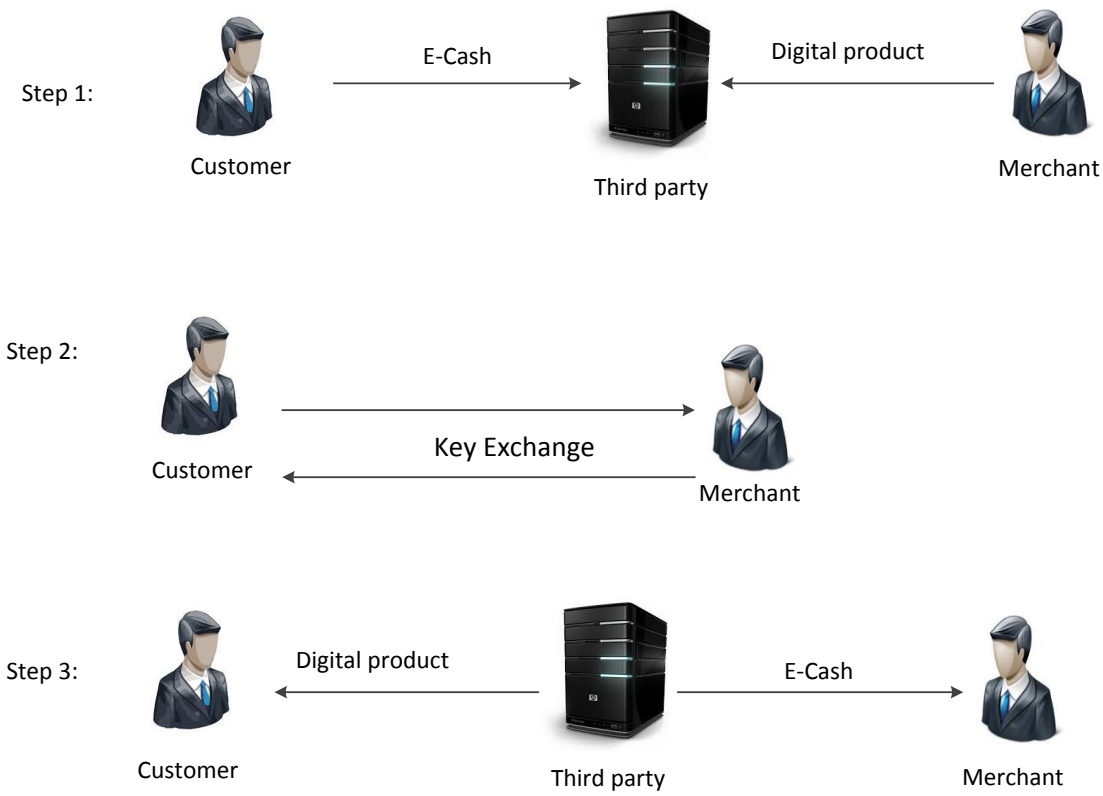


Fig. 5.27: Scenario 1 – Withdrawal Phase – Normal flow

Both the Merchant and the Customer then exchange the decryption keys and the Trusted Third Party sends the electronic cash to the Merchant and the digital product to the Customer.

Scenario 2: Both the Customer and the Merchant send the electronic cash and the digital product respectively to the Trusted Third Party but the Merchant wishes to withdraw from the transaction. In this case, the Merchant and the Customer would not exchange the decryption key, and hence, the second and the third step from the above diagram would not take place. Since the TTP does not have the decryption key, the electronic cash sent by the Customer can never be misused. The diagram below shows the flow described (Figure 5.28).

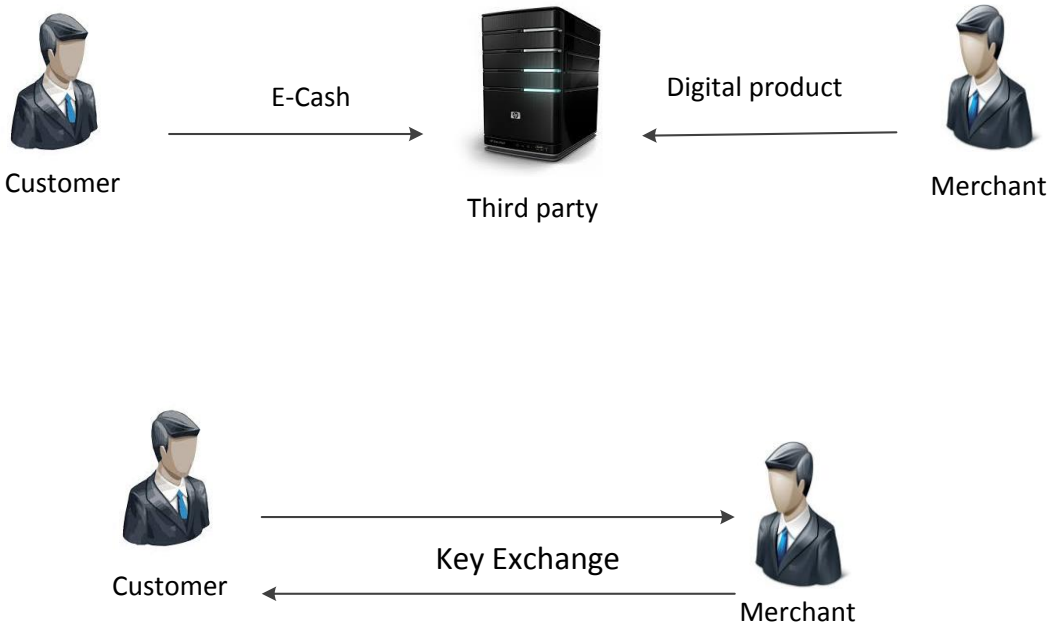


Fig. 5.28: Scenario 2 – Withdrawal Phase – Merchant wants to withdraw

Scenario 3: The Customer and the Merchant both send the electronic cash and the digital product respectively to the TTP but the Customer wants to withdraw from the transaction for some reason. In this case again, the Customer and the Merchant would not exchange the private decryption keys. The TTP will not be able to make use of the electronic cash or the digital product as there is no decryption key available. This is described in the diagram below (Figure 5.29).

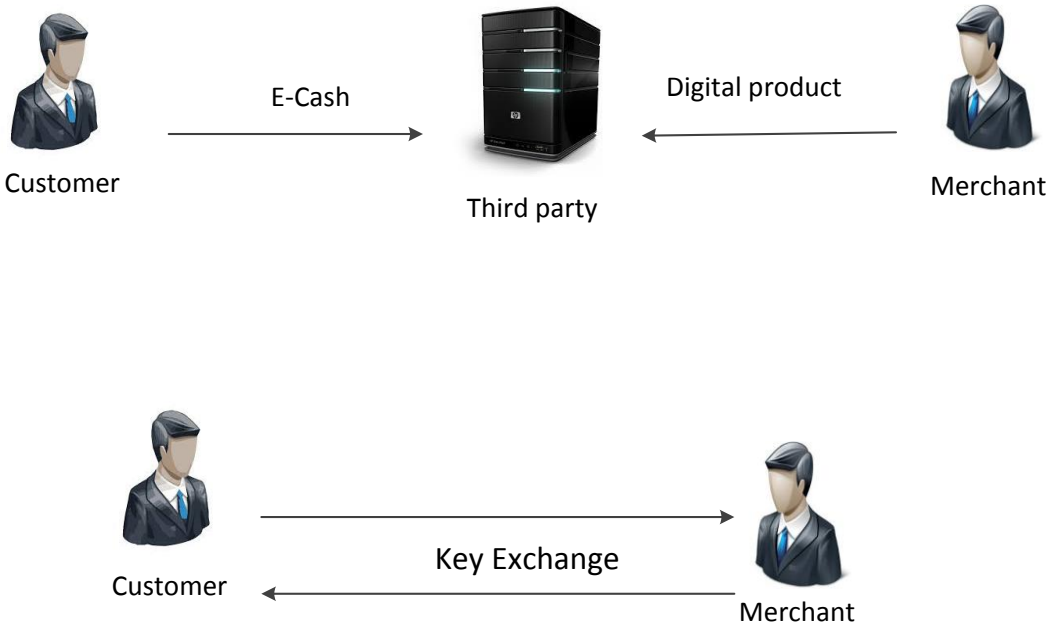


Fig. 5.29: Scenario 3 – Withdrawal Phase – Customer wants to withdraw

Scenario 4: The Customer and the Merchant have sent the electronic cash and the digital product to the TTP respectively and both of them now wish to withdraw from the transaction for various reasons. Similar to the above two scenarios, in this scenario, the Customer and the Merchant would not initiate the exchange of the private decryption keys. Without the decryption keys, both the electronic cash and the digital product is rendered useless in the hands of any other party. The diagram below (Figure 5.30) shows the flow mentioned here.

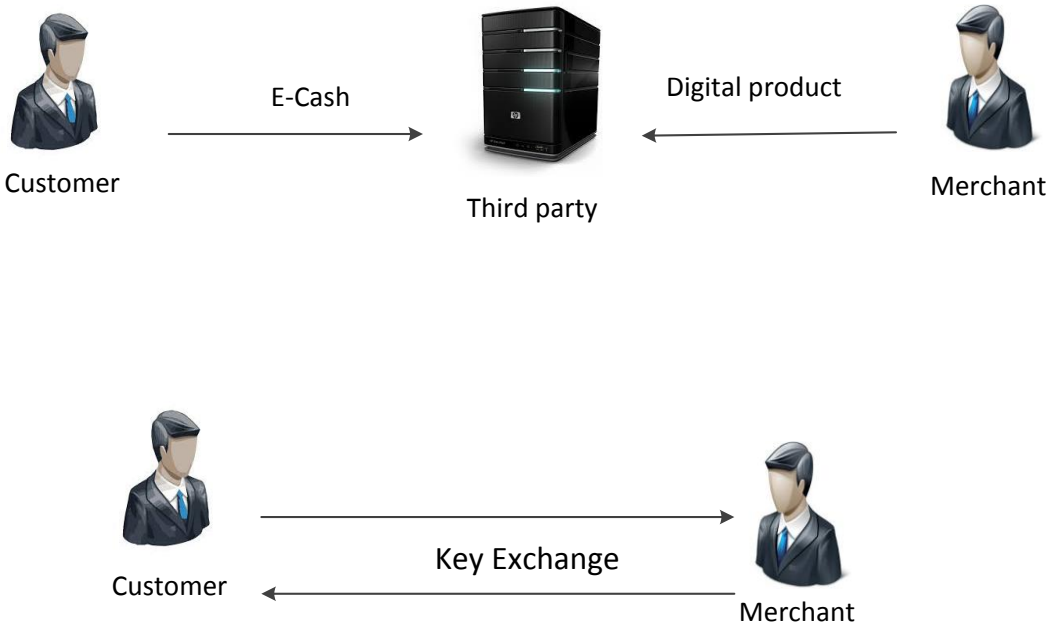


Fig. 5.30: Scenario 4 – Withdrawal Phase – Customer and Merchant want to withdraw

5.4 Summary

This chapter analysed the protocol based on various conditions that aimed to fulfil, including fair exchange and anonymity. Furthermore, areas that might lead to dispute were discussed in detail and identified the key areas where it becomes mandatory for the protocol or the parties involved in the e-commerce transaction to be able to easily detect dishonesty at different stages. From the analysis above, it is clearly understood that the protocol satisfies all the key aims, namely, fair exchange, provision of anonymity and payment security assurance. This is shown by highlighting all major scenarios and in certain cases all possible behaviours that could be shown by all of the transacting parties. Each scenario was then analysed and the result or the output detailing how the protocol would behave under each circumstance was described. In addition, from the above analysis, it can be clearly understood that, during a dispute, it is easy to identify the dishonest party and the reason for the dispute could be verified in a simple manner, as various scenarios and possibilities have been identified and explained in detail. Finally, a scenario analysis was conducted to see what happens when either or both parties are honest or

dishonest. This was demonstrated through a case-by-case example to determine if the detection of dishonesty was conducted in the correct manner by the protocol.

Furthermore, from the above sub-sections, it can also be understood that the protocol is designed in such a way where the number of disputes that might arise would also be minimal. This is because neither of the transacting parties, namely, the Customer and the Merchant, would receive the digital product or electronic cash before they sent the electronic cash or the digital product respectively, As the Trusted Third Party would only forward the items to the appropriate entities after receiving items from both parties. Furthermore, in the case of certificates and signatures, both the Merchant and the Customer can verify their authenticity before sending the digital product or the electronic cash respectively, as in order to forge a signature, the private key of the other party needs to be known. For example, if the customer wants to forge a signature on the electronic cash, then the customer would need to know the private key of the Bank that would be used to sign the electronic cash. Therefore, the question of incorrect or forged signature is impossible in this case.

Any failure in securing the communication channel is not a part of the protocol, and the protocol also does not describe any fail safe mechanisms or fault-tolerant techniques that could be adopted for the purposes of securing the communication channel. Hence, this is not within the scope of the protocol. Therefore, this area could be worked on in future development of the protocol.

The chapter also clearly demonstrated that there is a significant reduction in the number of actual messages between the Customer and the Merchant (which is restricted to two messages while they exchange the private decryption keys). The usage of an online Trusted Third Party is limited and is advantageous as the TTP does not need to be online full time. The TTP is also not involved in the key exchange process, which reduces the overheads of the TTP, making it more secure. Similarly, in case of disputes (all possible scenarios are clearly shown and discussed by the protocol), the number of messages required to resolve the issues are limited. In many cases, as indicated clearly in this chapter, the number of disputes arising is significantly reduced as fairness is imposed on the transacting parties of the protocol and no party involved in the e-commerce transaction (including the TTP) can take undue advantage of the other party/parties.

CHAPTER 6: PROTOCOL COMPARISONS

This chapter is aimed at comparing the proposed "Imposing Anonymity and Fairness Protocol" with various other similar protocols; that is, protocols that provide either anonymity or fair exchange, or both. This will help us to understand how efficient the proposed protocol is, and how it eliminates the gaps and/or deficiencies that are apparent in the other protocols.

Chapter Objectives:

- Enable the reader to comprehend the novelty of the proposed 'Imposing Anonymity and Fairness Protocol'.
- Understand the key differences in the protocols of similar nature, and clarify the contribution that the proposed protocol makes.
- Enable the reader to grasp how efficient the proposed protocol is, and to see how well it implements both anonymity and fair exchange. This will also help the reader to understand how the gaps mentioned in the literature are covered by this protocol.

6 Protocol Comparisons

The aim of this chapter is to compare the proposed protocol with the other protocols described earlier. This is done in order to understand how the protocol fares in terms of how well it overcomes the shortcomings of the other protocols discussed. It also aims at comparing the protocols' features and the overheads, and determining if the new protocol does better than the others. Also, only protocols with similar characteristics are compared here, to give a fair idea of how this protocol scores in comparison with those others.

In order to effectively compare the protocols, certain factors need to be taken into account against which the comparison is done. Accordingly, certain criteria used to make the comparisons, and these are as follows:

1. Number of messages
2. The requirement to hold data by the Trusted Third Party
3. Involvement of all the parties, namely the Customer (C), Merchant (M) and the Trusted Third Party (TTP), in case of dispute resolution

Furthermore, each protocol's disadvantage(s) is stated and is compared against the proposed protocol, to see whether or not the proposed protocol overcomes that disadvantage(s).

6.1 Number of Messages

The number of messages being exchanged throughout all the phases of the protocol plays a key role in determining the efficiency of the protocol. A large number of messages being passed between the transacting parties would mean that the protocol is complicated, and could become very cumbersome while being implemented. This is because 'messages' translate into 'time taken to process by the protocol', and during implementation, this also takes up a great deal of memory and processing space.

The proposed protocol is compared against the following protocols for the number of messages. These are:

1. Franklin & Reiter's Fair Exchange (with a semi-trusted Third Party) Protocol
2. Ray's Anonymous and Failure Resilient Fair Exchange E-commerce Protocol

3. Zhang's Efficient Protocol for Anonymous and Fair Exchange, and

Zhang's Mutual Authentication Enabled Fair Exchange and Anonymous E-payment Protocol

These four protocols provide both anonymity and fair exchange. The following table (Table 6.10) shows the number of messages in each protocol. The protocol becomes more efficient and effective when the number of messages are less. This is because, it makes it less cumbersome and while implementing the protocol, the amount of memory space required is less and the execution time is lessened resulting in a light-weight protocol. Hence the proposed protocol is better as seen from the table due to the lesser number of messages when compared to the other protocols.

Protocol	Number of Message
Franklin & Reiter	8 messages in the normal flow and 6 in the optimized protocol. This does not include the verification steps. Added with verification, it has a significantly large number of messages namely 10 in normal flow and 8 in the optimized flow.
Ray's Anonymous & Failure Resilient Protocol	10 messages
Zhang's Anonymity and Fair Exchange	10 messages
Zhang's Mutual Authentication Protocol	Total of 11 messages across 6 different phases.
Imposing Fairness Protocol	7 messages

Table 6.10: Number of messages

6.2 Requirement to Hold Data

This means that the Trusted Third Party would hold information that is being passed on between the two transacting parties, namely the customer (C) and the merchant (M). This sometimes leads to excessive space being used for storage and can create a bottleneck through having to secure the data being held by the TTP.

The following table (Table 6.11) shows the requirement to hold data by the TTP by the aforementioned protocols.

Protocol	Requirement to hold data
Franklin & Reiter	The TTP holds information for a short while for the purposes of verification.
Ray's Anonymous & Failure Resilient Protocol	Requires the TTP to hold data (the Merchant's item) before the exchange takes place.
Zhang's Anonymity and Fair Exchange	The TTP is required to hold data.
Zhang's Mutual Authentication Protocol	The TTP is required to hold data.
Imposing Fairness Protocol	The TTP is used only to hold data for a very short while, for the purposes of verification. All other messages are sent directly between the transacting parties.

Table 6.11: Requirement to hold data

6.3 Involvement of Parties during Dispute Resolution

This refers to what happens and which parties are involved in case of dispute resolution. This is an important aspect as, depending on the number of parties involved, it could become easier or more cumbersome.

The following table (Table 6.12) describes the involvement of parties during the dispute resolution phase for the four protocols mentioned.

Protocol	Involvement of parties
Franklin & Reiter	Only the party that is not happy along with the TTP.
Ray's Anonymous & Failure Resilient Protocol	All the transacting parties are involved in the dispute resolution phase.
Zhang's Anonymity and Fair Exchange	Only the party that is not happy, along with the TTP to provide an affidavit.
Zhang's Mutual Authentication Protocol	Only the party that is not happy along with the TTP.
Imposing Fairness Protocol	The dissatisfied party and the TTP are involved.

Table 6.12: Involvement of parties

6.4 Imposing Fairness vs. Franklin & Reiter's Fair Exchange Protocol

The disadvantages of Franklin & Reiter's Protocol and how the Imposing Fairness Protocol overcomes the same are listed in the table (Table 6.13) below.

Franklin & Reiter	Imposing Fairness Protocol
Semi-Trusted TTP	Partially trusted third party but controls in place to circumvent the TTP to read or modify messages
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

Table 6.13: Franklin & Reiter vs. Imposing Fairness

6.5 Imposing Fairness vs. Ray's Anonymous and Failure Resilient Protocol

The disadvantages of Ray's protocol are listed in the table below (Table 6.14) and it shows how the Imposing Fairness Protocol is designed to overcome the disadvantages mentioned.

Ray's Protocol	Imposing Fairness Protocol
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 bottleneck.	Anonymity is provided by means of using electronic cash and secure channels. This does not create any overheads.
Verification of the protocol by Kong et al. (2004) clearly shows that the TTP 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.
Provides only partial anonymity	Provides full anonymity

Table 6.14: Ray vs. Imposing Fairness

6.6 Imposing Fairness vs. Anonymity and Fair Exchange by Zhang

The table (Table 6.15) below lists the disadvantages of Zhang's Anonymity and Fair Exchange Protocol and compares it against Imposing Fairness Protocol.

Zhang's Protocol	Imposing Fairness Protocol
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 e-commerce transaction as demonstrated in Chapter 4.
Customers are required to disclose the public key during the transaction. Using the same key again and again might allow the merchants to trace the customer thus compromising the anonymity feature.	As electronic cash is being used, this is virtually untraceable and hence provides complete anonymity.

Table 6.15: Zhang's Anonymity & Fair Exchange vs. Imposing Fairness

6.7 Imposing Fairness vs. Zhang's Mutual Authentication Protocol

The table below (Table 6.16) 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	Imposing Fairness Protocol
Too many messages – 6 phases and 11 messages	Only 7 messages in total
It is very cumbersome as it has many phases.	The proposed protocol does not have iterative phases and hence is very efficient and fast.
It has a commit buffer that is used by the TTP 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 been thoroughly analysed to ensure it is available.

Table 6.16: Zhang's Mutual Authentication vs. Imposing Fairness

6.8 Summary

This chapter compared the proposed protocol with various other protocols. The comparisons (based on various criteria) clearly demonstrate that the proposed protocol fares a great deal better than all the other protocols, and effectively and efficiently overcomes their respective disadvantages. This clearly indicates the novelty of the protocol. Now that the protocol has been compared against the protocols, it is imperative to check the protocol's implementation that is discussed in the following chapter.

CHAPTER 7: PROTOCOL IMPLEMENTATION

The key goal of this chapter is to explain in detail the implementation of the "Imposing Anonymity and Fairness Protocol". This chapter provides a detailed report on the software framework that has been used, discusses the need to implement the protocol, describes the various modules that are present in the protocol's implemented prototype, and also explains the key features of the prototype. It concludes by identifying areas for improvement or enhancements that could be made to the protocol's prototype.

Chapter Objectives:

- Enable the reader to understand the need to implement the proposed protocol as a software prototype.
- Justify the selection of the programming language and the interface that has been used to implement the prototype.
- Enable the reader to grasp the key features of the implemented prototype and also to identify the shortcomings of the prototype that is being developed.
- Help readers get an idea about the different software modules within the prototype and how these software modules communicate with each other effectively and efficiently.

7 Protocol Implementation

To further understand the performance of the protocol, it is implemented as a prototype. This will assist in evaluating the protocol and the results that it generates will be illustrated in a more visually appealing manner. The implementation of the proposed protocol serves as one of the verification and evaluation methods as discussed in the previous chapters. The main aims of having an implementation of the proposed protocol are as follows:

1. To demonstrate that the protocol that is proposed is ready to use in the real world and can be extended to run on a client-server environment.
2. To further understand the time it takes for the protocol to actually execute and to identify areas that need to be modified; in simple terms, it aims to identify the key areas of concern or those areas that affect the performance of the protocol, to ensure that these areas are redesigned or revisited.

7.1 The Prototype

The prototype is an implementation viewpoint of the proposed e-commerce protocol. It enables thorough testing of the protocol once it is implemented, to identify any key flaws in the logic, design or data and/or system flows. The prototype is implemented using a web service based Java Enterprise Edition. The key features of this prototype display the main functions and show all the key entities responsible in an e-commerce transaction. In simple terms, it represents the key participants or the core functions in the proposed e-commerce protocol.

1. A server side Java EE application for the Trusted Third Party (TTP).

2. A client side web interface to access and validate hashes with the TTP. This web interface is accessible to both the Customer (C) and the Merchant (M).

3. A server side Java EE application for the Certificate Authority (CA).

4. A client side web interface to access and validate the hashes with the CA. This client interface is accessible to both the Customer and the Merchant.

5. A server side Java EE application for the Customer Bank (CB).

6. A client side web interface to withdraw and validate digital cash with the CB. This web interface again is accessible to both the Customer and the Merchant.

The whole prototype is deployed in a single server (for testing purposes). The prototype is designed in such a way that it could be made fully responsive and suitable for mobile applications. The prototype that has been developed using Java can be divided into two key parts. These are:

1. The Kernel: this acts as the 'central module' that loads during the initial stages of the protocol and remains constantly in the memory. It provides all the key services that are required by various other modules in the prototype and enables the smooth running of the prototype.
2. Application Modules: these modules represent the various entities in the proposed protocol, namely C, M, CA and TTP. These application modules have the capability to communicate with each other.

In simple terms, the kernel is something that would act as the core or the crux of the program. The main function of this part is to ensure that all required modules are loaded correctly and to make sure that the Java program is running without any glitches.

The figure below (Fig. 7.31) describes the structure of the Application Module as well as the components and structure of the key computational modules.

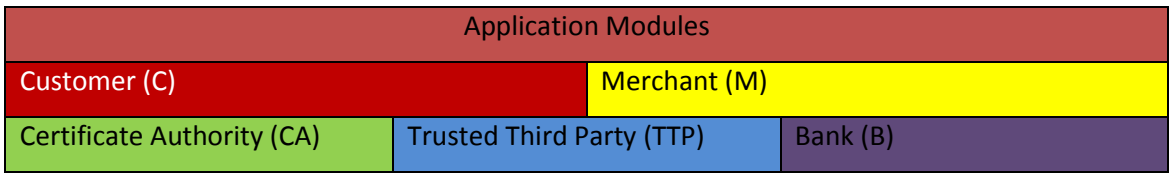
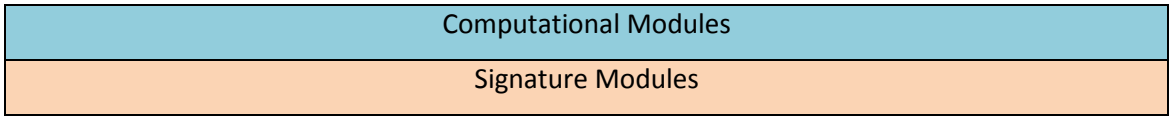


Fig. 7.31: Components of the application modules

As mentioned, there are five application modules and these have the ability to communicate with each other.



Cryptographic Modules	Hash Modules
Java Cryptographic Application Programming Interfaces (APIs)	
Java Runtime Environment (JRE)	

Fig. 7.32: Components of the key computational modules

The computational modules are those modules without which the program cannot run. The APIs and the JRE are automatically provided by the Java programming language. The remaining three modules are common modules that could be used by any of the application modules.

It is also important to understand that these two key modules, i.e. the application modules and the computational modules, communicate with each other. For example, if the Customer wants to send hashed and encrypted cash to the Trusted Third Party, the Customer Module will make use of the Cryptographic Modules and the Hash Modules to be able to hash and encrypt the cash in order to send it to the TTP.

The Java Enterprise Edition system architecture is depicted in the diagram below (Fig 7.33)

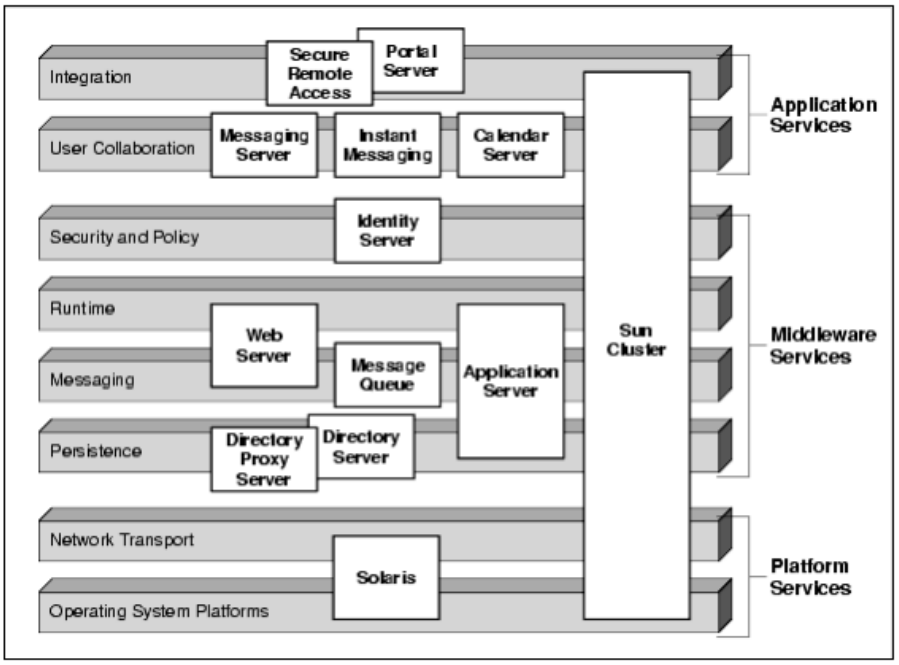


Fig 7.33 Java Enterprise System Architecture (Source: Oracle, 2014)

From the above diagram, it is clear that the enterprise edition provides platform services, middleware services as well as application services in order to support the web application that is being developed.

This implementation uses a three-tier logic whereby the clients or the end users make calls to specific business tier logic components or Java Modules which internally communicate to the web services and servers. At the back end the databases are present which can be accessed by the business logic tier. This is depicted in the diagram below (Fig 7.34)

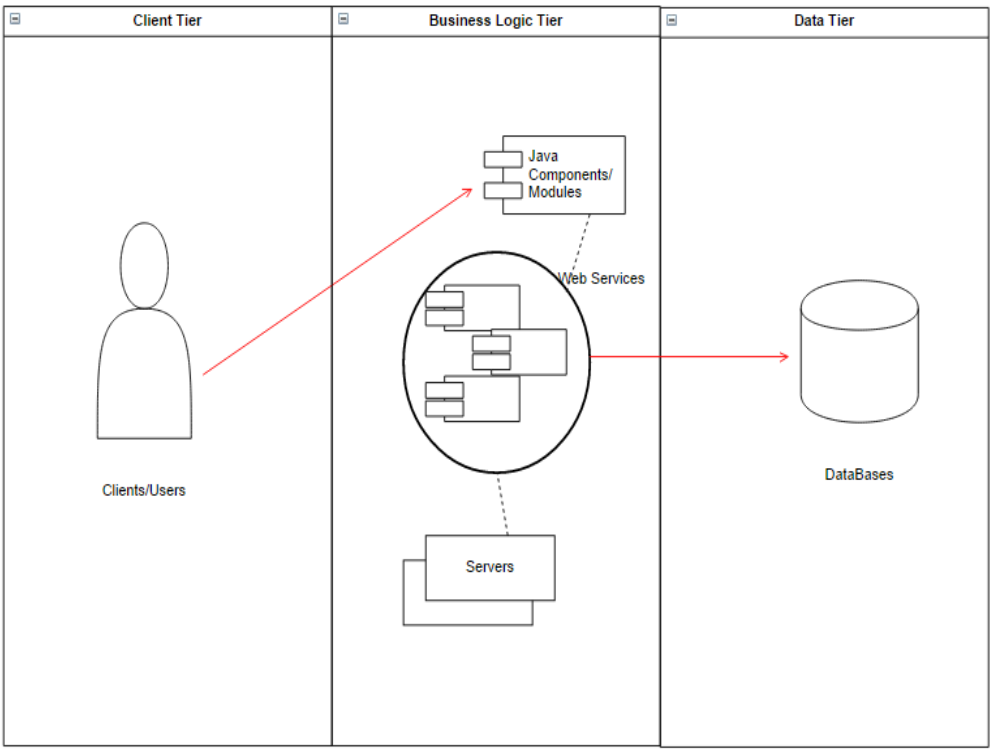


Fig 7.34 Implementation Design Logic

The five key components namely the client, merchant, Trusted Third Party, Certificate Authority and Merchant Bank communicate with each other during an e-commerce transaction either by a web interface which is depicted in the diagram below (Fig 7.35)

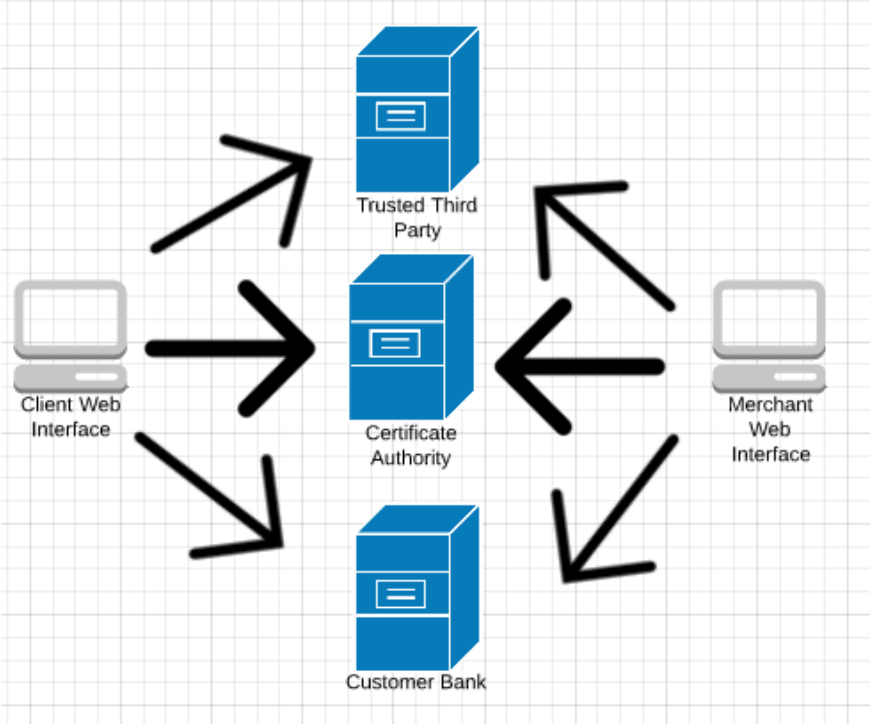


Fig: 7.35: Interaction between components

7.1.1 Kernel Component

This section aims at describing in detail all the modules within the Kernel Component of the prototype. This component has four key modules. These are:

1. Hash Module
2. Cryptographic Module
3. Signature Module, and
4. Computational Module

7.1.1.1 Hash Module

This module is used to compute all the hashes that are used by the prototype. For example, this module is called when the Customer wants to hash the message before sending it to the TTP. It services all of the layers within the application module. In simple terms, this module can be called by any of the modules within the application layer. When any of the modules within the application layer require messages to be hashed, this module is called. This function works by taking a variable-length string, which is known as the pre-image, processes it using the hash function and outputs a fixed-length string, which is known as the hash value or a cryptographic

checksum. Whatever the length of the input, the size of the output remains constant. The hash function used in this prototype is SHA-1. The SHA-1 algorithm that is used in this module (Secure Hash Algorithm - 1) uses a 512 bit block size for hashing. The process is as follows:

The message is broken down to 512 bit blocks. The message is then padded with one followed by zeros so that there are 448 bits in the final block of the message.The original message is then appended as an unsigned 64 bit integer. The method given in SHA-1 Manual (NIST, 2013) is followed whereby 5 blocks of hash are initialised (h0, h1, h2, h3 and h4) and an internal loop is used to calculate the hash and a final block of 160 bits is output.

7.1.1.2 Cryptographic Module

The cryptographic module is one of the key modules that would be called upon to perform any cryptographic functions (except hashing and digital signature). In a gist, this includes encryption and decryption of messages, producing timestamps, generating key pairs, etc. The key functions of this module are as follows:

1. Generate symmetric key pairs for encryption with AES (Advanced Encryption Standards). The block size is 128 bits.
2. Perform the function of symmetric encryption and decryption. This is done by taking the symmetric key that has been generated and performs the appropriate function of encryption or decryption as required. Again, AES is used by this function and the block size in use is 128 bits.
3. Perform the function of asymmetric encryption. Asymmetric encryption, as discussed in the earlier chapter makes use of two keys (unlike symmetric key cryptography), a private and public key. The keys are RSA-based.
4. Perform the function of asymmetric decryption. This is done by making use of the private and public keys that are generated (based on the RSA algorithm).

7.1.1.3 Signature Module

This module is used for all signing purposes for any digital signatures. It makes use of two other modules, namely the hash module and the cryptographic module, to integrate different inputs and output a digital signature. It is used for the following purposes:

1. Produce a digital signature: this makes use of a signing function whereby the private key of the signer is taken to sign the hash value of any message. This signed hash using the

private key on a message represents the digital signature of the signer. This module can be used by the transacting parties only if they know the private key.

2. Verify the digital signature: to verify a signature, this function makes use of the signer's public key. This is used to decrypt the message. After the message is decrypted, the hash value of the original message is calculated. Once this is done, this value is compared with the hash value of the decrypted signature. This helps in verifying the signer of the message. Any discrepancy in the hash values would mean that the signature has been forged by the sender.

7.1.1.6 Computational Module

This module is developed to service all layers in the Kernel Module below it. In short, it would perform all requests from the Signature Module, Hash Module and the Cryptographic Module. The main functions carried out by this module would include all mathematical operations that would be needed for the other modules to perform their operations. These mathematical operations, for example, might include:

1. Generation of random numbers for computing the RSA keys.
2. Performing basic the mathematical operations that are required for encryption or decryption.

7.1.2 Application Modules

The application modules represent the key entities that are involved directly or indirectly in the e-commerce transaction. This module communicates with the underlying kernel layer to enable the computation and processing of requests. This module enables communication with each of the sub-modules or layers, and assumes that all interactions between the modules are secure. This module consists of the following layers:

1. Customer
2. Merchant
3. Trusted Third Party
4. Certificate Authority
5. Bank

7.1.2.1 Customer

The Customer Module enables the Customer to do the following:

1. View the products that are displayed on the Merchant's site.
2. Verify the digital certificate provided by the Merchant through the Certificate Authority.
3. Withdraw electronic cash from the Bank.
4. Communicate interest in buying to the Trusted Third Party.
5. Show proof of funds to the TTP.
6. Exchange keys with the Merchant.
7. Decrypt the electronic product purchased.

The customer can also withdraw from the transaction by not sharing the decryption key with the Merchant.

7.1.2.2 Merchant

This module is developed for the Merchant to facilitate the Merchant in carrying out the following functions:

1. Obtain a digital certificate from the Certificate Authority to confirm the online identity and to improve the customers' perception of trust.
2. Upload digital products online for potential customers to view and purchase.
3. Verify with the Customer's bank the authenticity of the electronic cash.
4. Communicate with the Trusted Third Party and send the encrypted product to the TTP.
5. Exchange keys with the Customer for decryption.
6. Decrypt the electronic cash.

7.1.2.3 Trusted Third Party

This module assists in facilitating the Trusted Third Party to perform various key activities. These activities include the following:

1. Verify the authenticity of the digital product and the electronic cash that has been sent by the Merchant and the Customer, respectively.
2. Mediate between the Customer and the Merchant as and when necessary.
3. Store records of transactions in case of any disputes.

4. Send the digital product and the electronic cash to the Customer and the Merchant, respectively, after they have exchanged the keys.

7.1.2.4 Certificate Authority

This module enables the Certificate Authority to perform the following key tasks:

1. Issue a digitally signed certificate to the Merchant after verifying the Merchant's identity in the pre-exchange or the pre-negotiation phase of the e-commerce transaction.
2. Verify any certificates issued on request from the Customer or the Trusted Third Party. This is done by maintaining a list of certificates issued earlier.

7.1.2.5 Bank

This module enables the Bank to perform the following activities:

1. When the Customer requests electronic cash, check the account of the Customer to ensure that there are adequate funds.
2. On confirming funds, either issue the electronic cash or a rejection due to lack of funds.
3. Ensure that the electronic cash is not double spent or forged by checking the database of spent cash and verifying the blind signature.
4. On request from the merchant, to deposit the electronic cash after the e-commerce transaction, and process the request.

The following diagram (Fig. 7.36) clearly depicts the communications between all the modules in the application layer of the protocol:

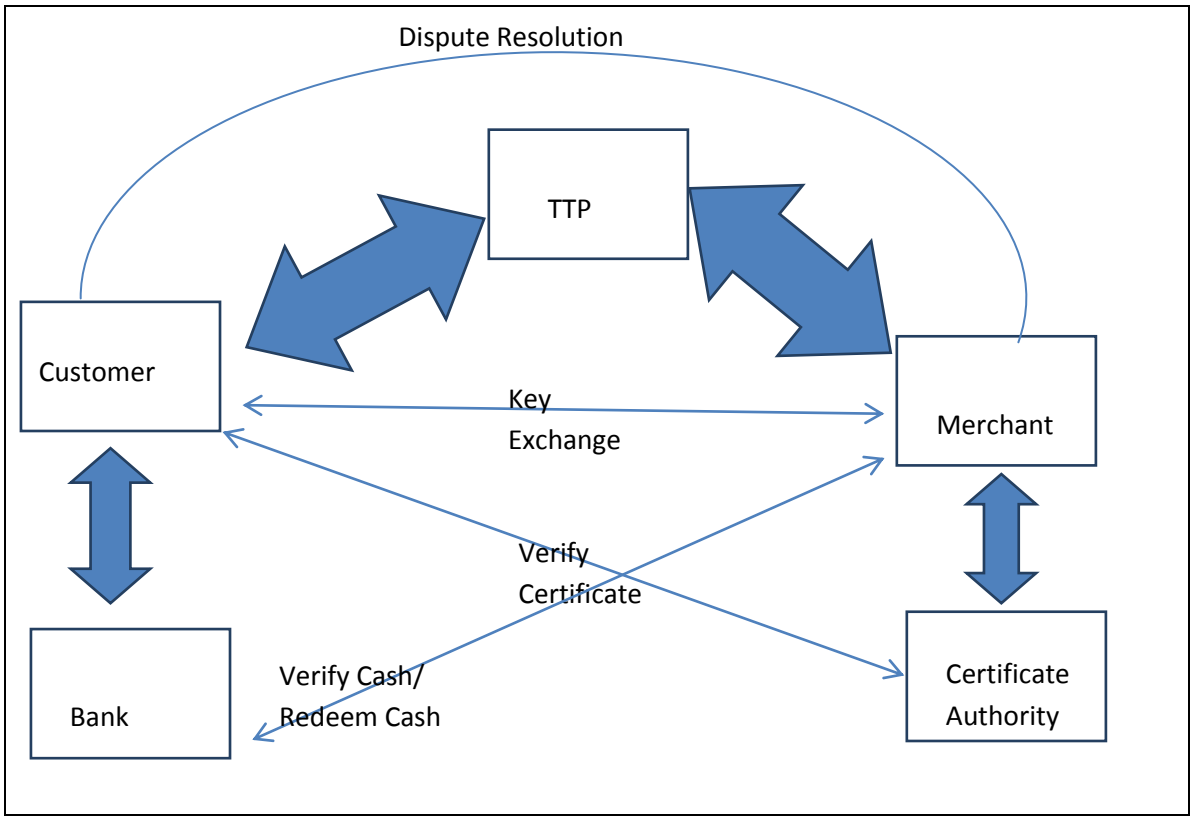


Fig. 7.36: Communication process between all modules in the application layer

Each module in the application layer is defined as a 'class' in the actual Java program. Each class contains many objects. The objects of a class have attributes and behaviours associated with them. Communication between the classes happens by making use of the objects. For example, in this case, Customer is a class. The class has various methods that define what the Customer can do. For example, the methods of the Customer class include View Product, Send Cash, and so on. Each and every individual customer is an object of the class Customer. Methods define what the class can do. In short, these define the capability of the class to perform certain actions.

For example, if the customer wants to encrypt, hash and timestamp the e-cash before sending it to the TTP, the customer first calls the cryptographic module to encrypt the message. For the purposes of encryption, the cryptographic module first generates a symmetric key pair with Advanced Encryption Standards with a 128 bit block size. To divide the message to the blocks, the cryptographic module calls on the computational module to perform this function.

Once the blocks are obtained, the AES function within the cryptographic module (or class) is used to encrypt the data and this is sent back to the customer. The customer then calls on the hash module with the encrypted message to provide a hash. The hash module then calls the computational module to divide the message into blocks and then performs the hash. This 160 bit hash is then passed on to the customer. The customer would now need to call the signature module to digitally sign the message. The signature module then calls the cryptographic module to obtain the private key of the customer and then the hash method to hash the private key to obtain the signature. When the cryptographic module is called to obtain the private key, it internally uses the RSA algorithm to generate the public-private key pair. The RSA method, in order to generate the key pairs would need to call the computational module to perform operations such as random number generation etc. This example is depicted in the diagram below (Fig 7.37)

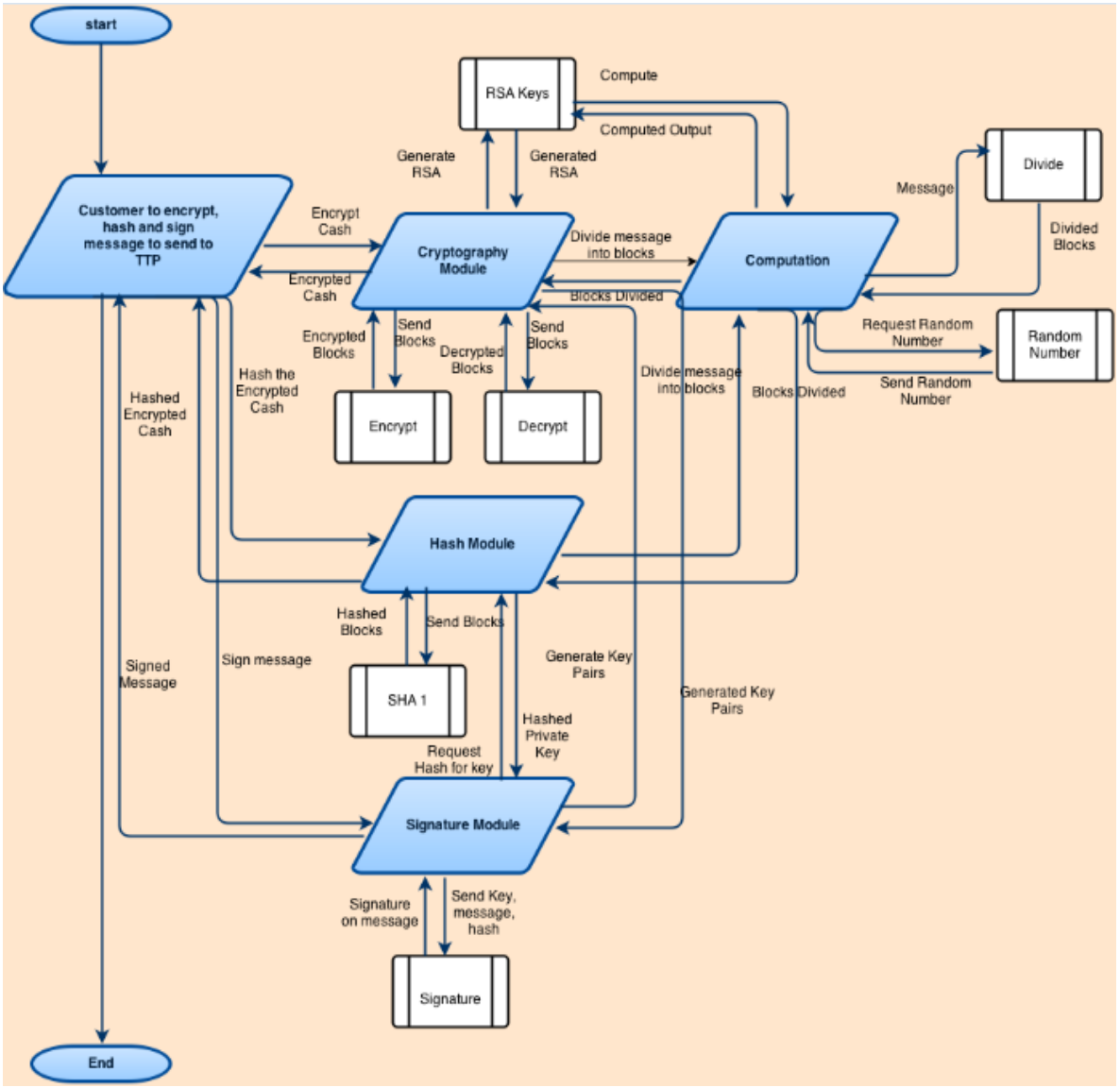


Fig 7.37: Example of Customer encrypting, hashing and signing a message

7.1.3 Future Developments

The aim of this prototype was to provide a very basic functionality to the protocol in order to test its readiness to be implemented in the real world. Hence, there are many areas that could be considerably improved, keeping in mind the latest technologies available.

This prototype therefore is not production ready, but for all intents and purposes perfectly suitable for testing. Also, there is no authentication and it may be error-prone on some occasions, as Test Driven Development (TDD) was not used. One of the key assumptions is that

everything in the forms is filled correctly. Given these drawbacks, the following could be done for further enhancement of the protocol's prototype:

1. Automatic decryption of the product after the final stage of the protocol. Trusted Third Party asks if the customer wants the product to be decrypted by the TTP server for him. The button is already there in the TTP interface.
2. Full-blown X.509 security stack with run-time certificate issuing and revocation. At the moment, the prototype does not deal with certificate revocation. However, in the real world, the Certificate Authority is required to maintain a list not only of the certificates issued but also of the certificates revoked. This is known as the Certificate Revocation List. This is also done in real time and updated as and when the certificates are issued and/or revoked.
3. Proper authentication and authorization. This could be done by using an appropriate login and password for all the parties. This has not been implemented in the prototype as the security of the individual parties is not within the scope of the protocol.
4. Merchant's view on placed orders and their payment states. This could be done to enhance the user experience. This shows the list of all recent orders that are placed by customers, the status of payment (whether or not payment has been received, whether or not the electronic cash is redeemed from the bank, et cetera).

Also, it needs to be understood that although the protocol's implementation is fully functional, it is in a very raw form; it needs to be modified to enhance and appreciate the protocol thoroughly. This means that the prototype only provides the basic services and implements only the two layers mentioned above (namely the kernel and the application), i.e. it does not provide any additional features to improve the experience and cannot be used as a substitute to a full-blown implementation-ready application. Also, the protocol does not exactly use X.509 certificates; rather, it just uses RSA key pairs, just like the X.509 certificates, to simulate the X.509 stack. Improvements would also enhance the user experience but this is not within the scope of this implementation. This implementation has proved that the protocol is feasible; it is a simple means to verify the outputs and also to show that the logic followed is correct.

7.2 Message flows in the prototype

The prototype is done with the intention of showing the readiness of the protocol in the real-world. It helps to show that the protocol is a robust model that could be implemented and adapted to different platforms for Business-to-Consumer electronic commerce transactions. The prototype is created with the intention of proving that the protocol's logic works fine. Based on these, the following are the key assumptions that have been followed while developing the prototype:

1. There is only one Merchant and his name is "Merchant". Though the protocol allows having multiple merchants, the prototype was created with the intention of showing the logical flow. Hence only one Merchant was used. Similarly only one Bank is being used for the purposes of simplicity and ease.

2. All prices are denoted in terms of integers. Though in the real-world prices could be both integers and decimals, for implementation purposes, it is assumed that the prices are integers.

3. The implementation of the prototype does not provide for any error correction as it is assumed that the forms are filled up in the correct manner. Validation on individual text fields is not present as the purpose is to demonstrate the logical flow of the protocol and not the implementation itself.

The prototype does not provide a page specifically for the customer as it is designed from the point of view of the customer. The bank page provides a list of the customers. It provides an interface to withdraw digital payments and also to perform other banking related transactions. The banker can add new customers and the account details. A payment can be generated in the bank's website by selecting the banking client from the list and filling the form with the payee details. Given that we have only one Merchant, the payee would always be "Merchant" in this case. The price of the product could be filled in depending on the amount to pay. The diagram below (Figure 7.38) shows the bank client interface.

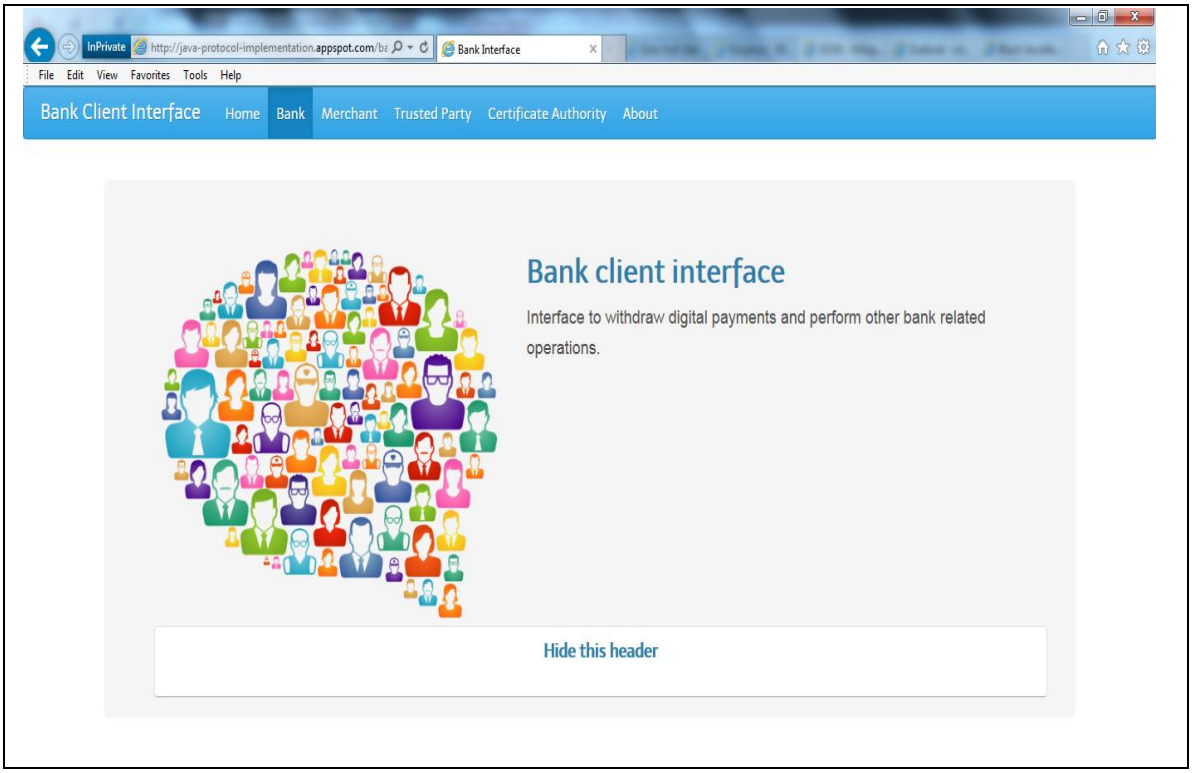


Figure 7.38: Bank Client Interface

Once Generate button is pressed, it generates a digital code for the payment to be made. It gives the hash of the payment to be checked at a later stage (to ensure integrity of the payment), the encrypted hash (for confidentiality purposes) and the private key that needs to be shared with the merchant. A JSON for the Payment is also generated at this stage which the customer can now make use of to make the payment for the desired product. This is depicted in the figure below (Figure 7.39)

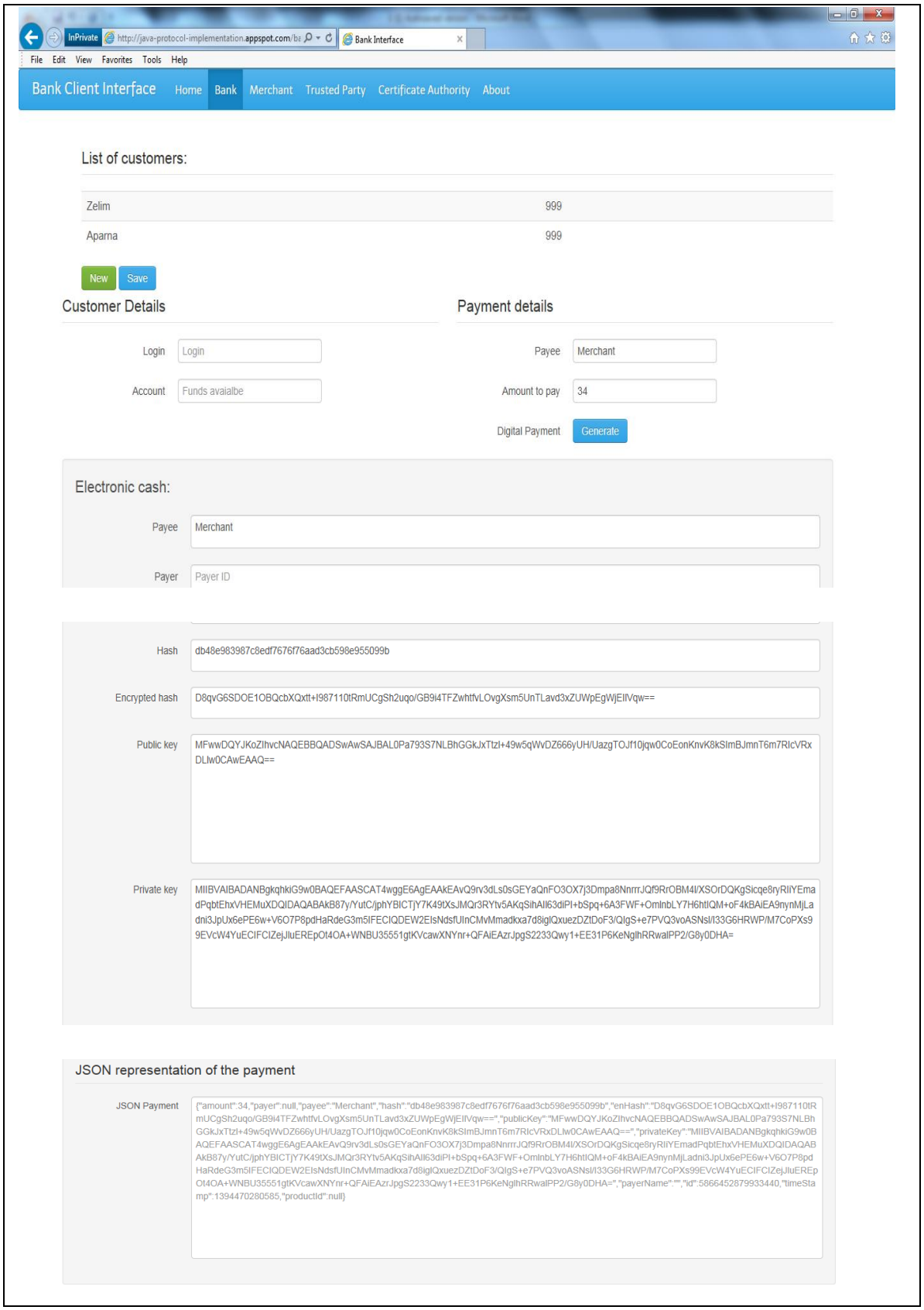

InPrivate
http://java-protocol-implementation.appspot.com/ba
Bank Interface
File Edit View Favorites Tools Help
Bank Client Interface
Home
Bank
Merchant
Trusted Party
Certificate Authority
About
List of customers:
Zelim 999
Aparna 999
New
Save
Customer Details
Login
Account
Payment details
Payee
Merchant
Amount to pay
34
Digital Payment
Generate
Electronic cash:
Payee
Merchant
Payer
Payer ID
Hash
db48e983987c8edf7676f76aad3cb598e955099b
Encrypted hash
D8qvG6SDOE1OBQcbXQxtt+I987110tRmUCgSh2uqo/GB9i4TFZwhtfvLOvgXsm5UnTLavd3xZUWpEgWjEIIVqw==
Public key
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL0Pa793S7NLBhGGkJxTtzI+49w5qWvDZ666yUH/UazgTOJf10jqw0CoEonKnvK8kSImBJmnT6m7RlcVRxDLIw0CAwEAAQ==
Private key
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAvQ9rv3dLs0sGEYaQnFO3OX7j3Dmpa8NnrrrJQf9RrOBM4I/XSOrDQKgSicqe8ryRIiYEmadPqbtEhxVHEMuXDQIDAQABAkB87y/YutC/jphYBICTjY7K49tXsJMQr3RYtv5AKqSihAII63diPI+bSpq+6A3FWF+OmlnbLY7H6htIQM+oF4kBAiEA9nynMjLadni3JpUx6ePE6w+V6O7P8pdHaRdeG3m5IFECIQDEW2EIsNdsfUInCMvMmadkxa7d8iglQxuezDZtDoF3/QIgS+e7PVQ3voASNsl/I33G6HRWP/M7CoPXs99EVcW4YuECIFCIZejJluEREpOt4OA+WNBU35551gtKVcawXNYnr+QFAiEAzrJpgS2233Qwy1+EE31P6KeNglhRRwalPP2/G8y0DHA=
JSON representation of the payment
JSON Payment
{"amount":34,"payer":null,"payee":"Merchant","hash":"db48e983987c8edf7676f76aad3cb598e955099b","enHash":"D8qvG6SDOE1OBQcbXQxtt+I987110tRmUCgSh2uqo/GB9i4TFZwhtfvLOvgXsm5UnTLavd3xZUWpEgWjEIIVqw==","publicKey":"MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL0Pa793S7NLBhGGkJxTtzI+49w5qWvDZ666yUH/UazgTOJf10jqw0CoEonKnvK8kSImBJmnT6m7RlcVRxDLIw0CAwEAAQ==","privateKey":"MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAvQ9rv3dLs0sGEYaQnFO3OX7j3Dmpa8NnrrrJQf9RrOBM4I/XSOrDQKgSicqe8ryRIiYEmadPqbtEhxVHEMuXDQIDAQABAkB87y/YutC/jphYBICTjY7K49tXsJMQr3RYtv5AKqSihAII63diPI+bSpq+6A3FWF+OmlnbLY7H6htIQM+oF4kBAiEA9nynMjLadni3JpUx6ePE6w+V6O7P8pdHaRdeG3m5IFECIQDEW2EIsNdsfUInCMvMmadkxa7d8iglQxuezDZtDoF3/QIgS+e7PVQ3voASNsl/I33G6HRWP/M7CoPXs99EVcW4YuECIFCIZejJluEREpOt4OA+WNBU35551gtKVcawXNYnr+QFAiEAzrJpgS2233Qwy1+EE31P6KeNglhRRwalPP2/G8y0DHA=","payerName":"","id":586645287993344,"timeStamp":1394470280585,"productId":null}

Figure 7.39: Payment Generation by Bank

Now, the customer can go to the merchant page (which represents the merchant's website in the real-world) and choose the desired product. The customer can choose to verify the product with the Certificate Authority by using the "Verify" option that is available. When the customer clicks on the buy option, the customer is redirected to the Trusted Third Party website. The details of the product would automatically be populated and the customer is just required to paste the copied JSON code on the text area that is provided and press the "Parse JSON" button. The figure below shows the Merchant's website (Figure 7.40) from a point of view of the customer.

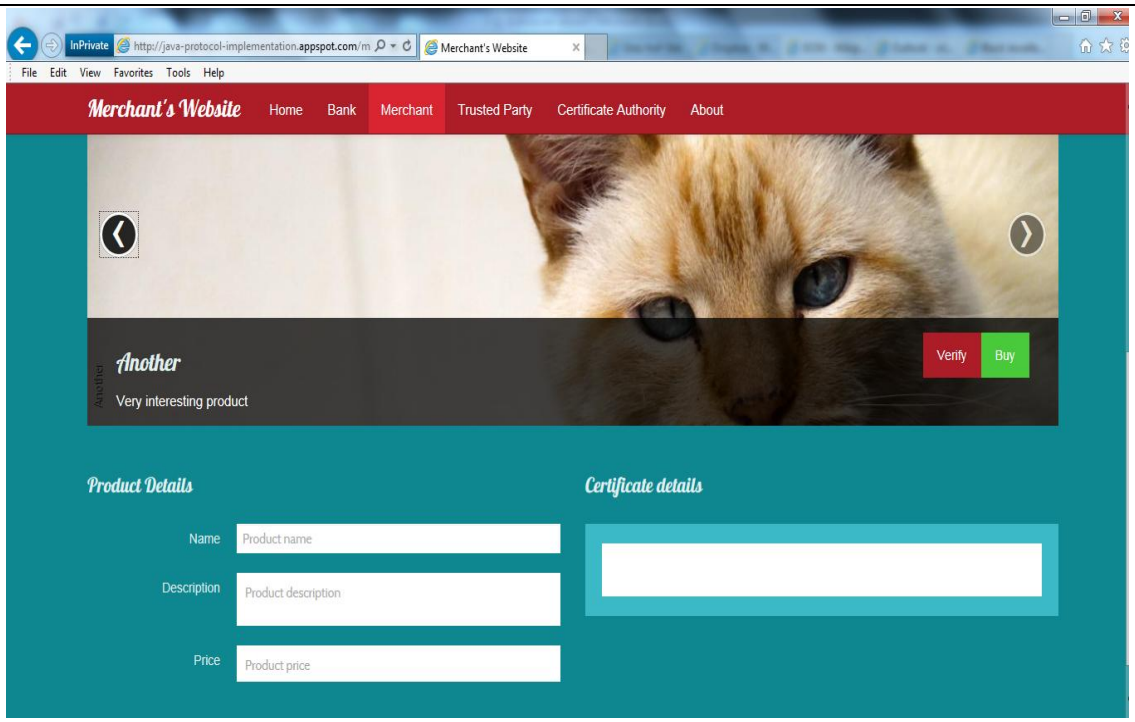


Figure 7.40: Merchant website from the point of view of the customer

The figure below (Figure 7.41) shows the redirection to the Trusted Third Party website when the customer clicks on the buy option. The trusted third party site is used by both the customer and the merchant.

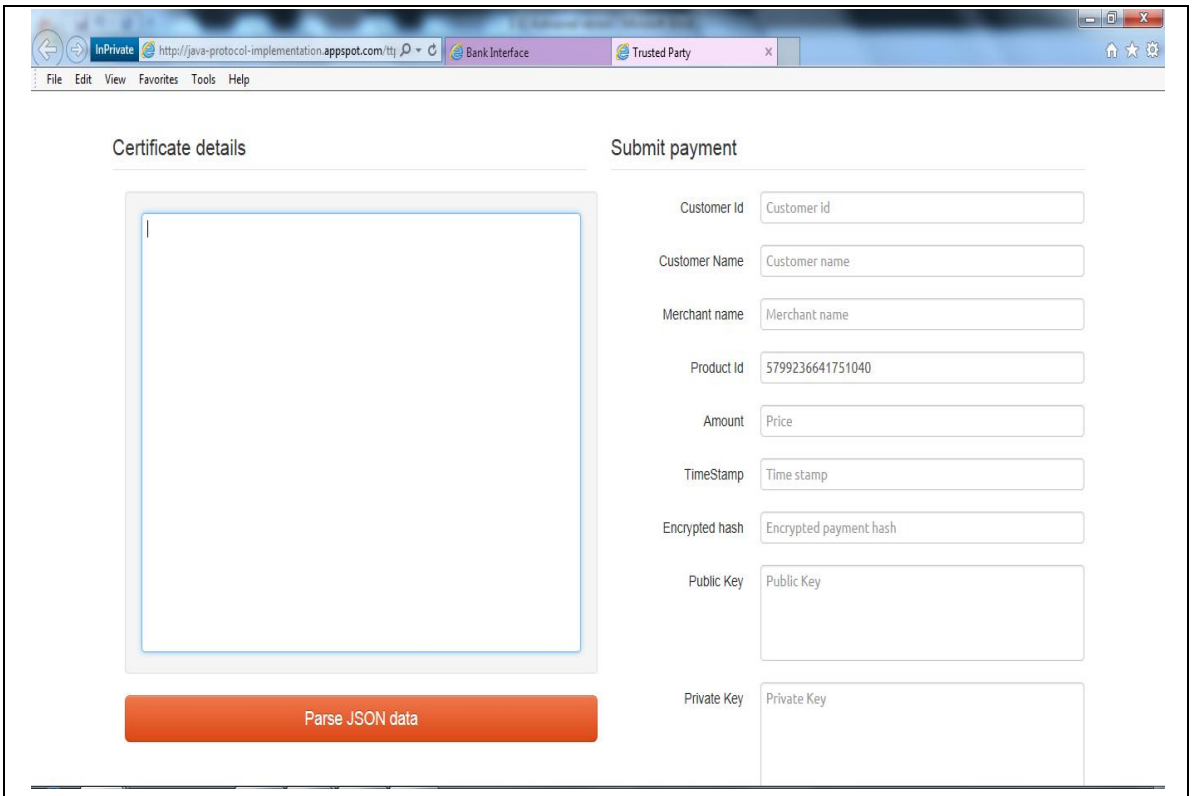


Figure 7.41: Trusted Third Party website for Customer

The customer can then click on the initiate protocol button. This leads to the protocol generating the encrypted contents of the product. The customer can now click on make payment (or verify with CA before making the payment to ensure that the product is legitimate). When the customer clicks on the verify button, he/she is redirected to the Certificate Authority's page where the verification status is shown. The figure below shows the verification screen for the product (Figure 7.42)

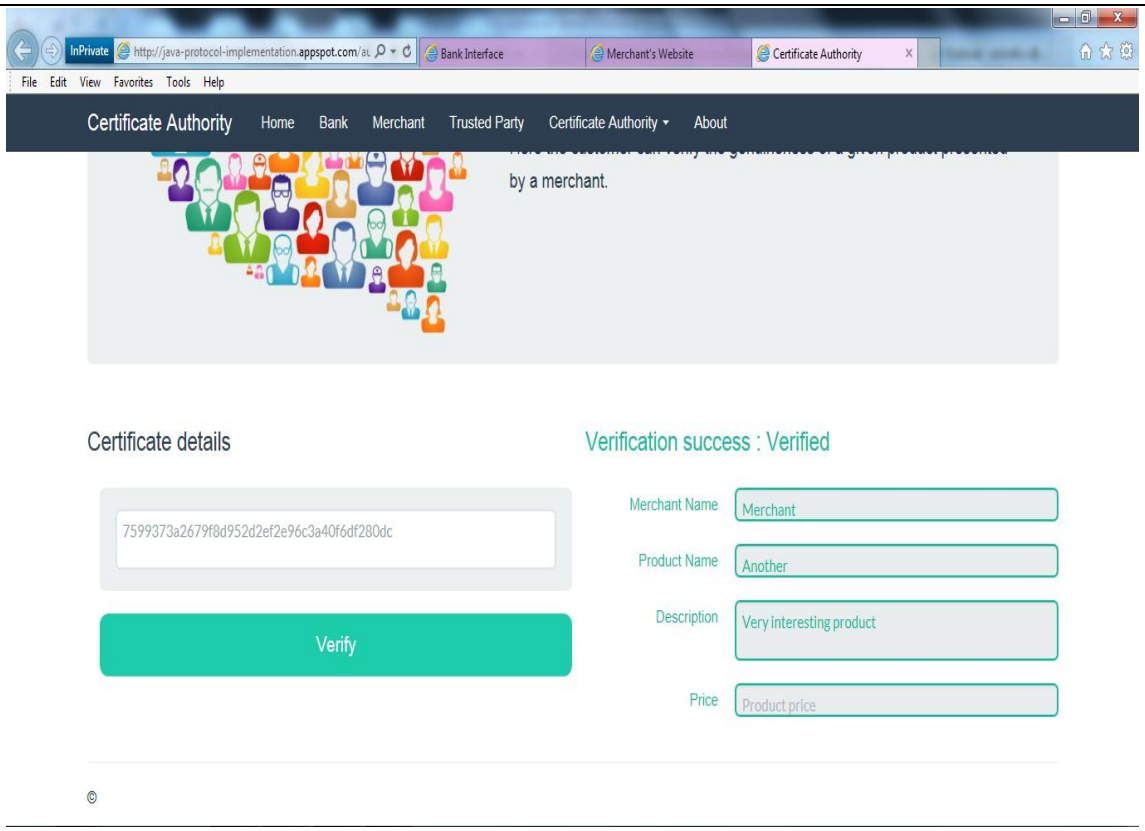


Figure 7.42: Product Verification by Certificate Authority

Once the make payment option is clicked, the private key that has been generated can now be used to decrypt the product contents. Similarly, the merchant would be able to use the key to decrypt the payment and withdraw cash from the Bank.

Now, from the Point of view of the merchant, the following happens. First, the Merchant goes to the Certificate Authority's page and adds the desired product including the product name, contents, price and clicks the certify option. This generates the certificate for the product added. This is depicted in the diagram below (Figure 7.43)

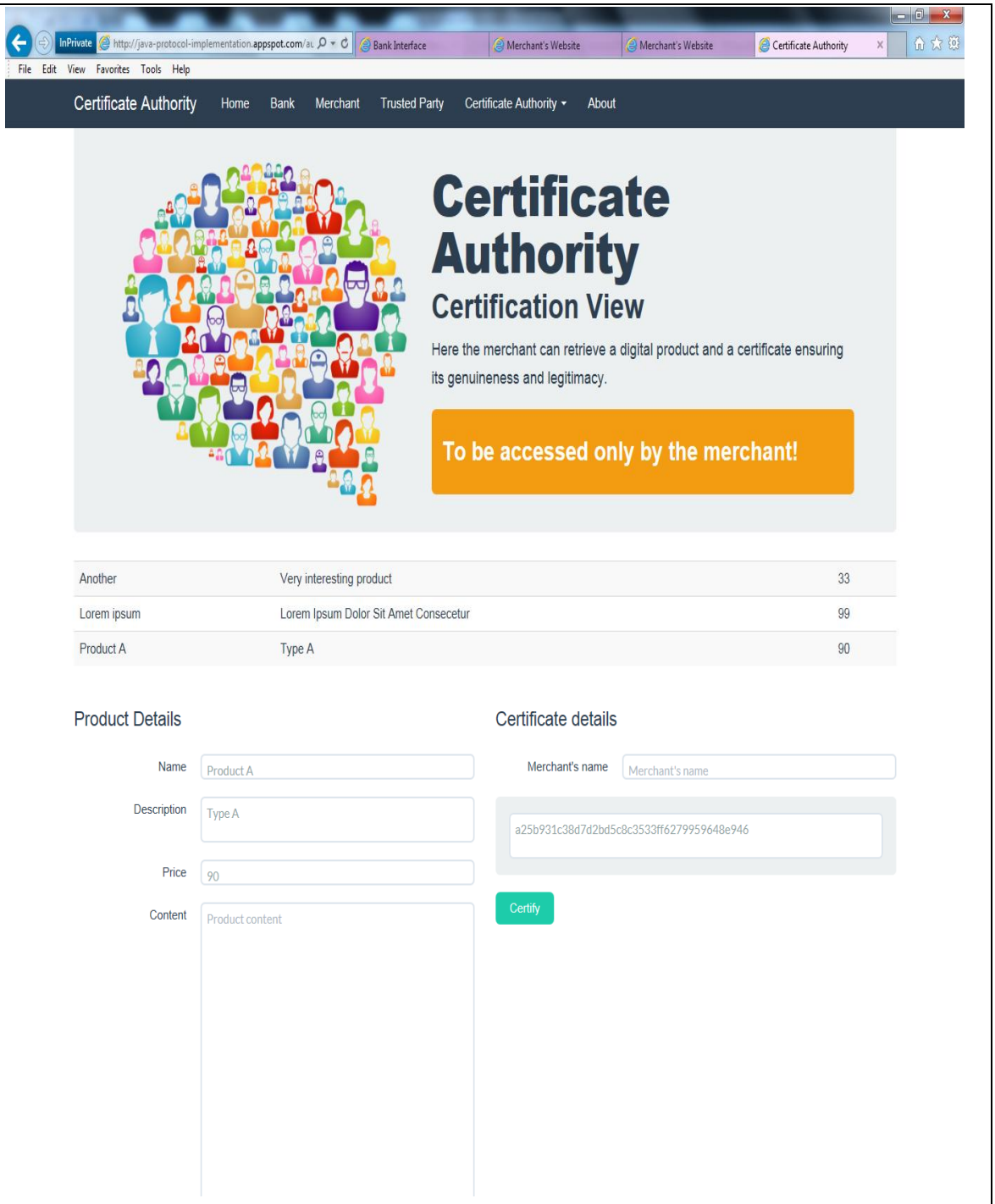


Figure 7.43: Merchant getting a product certified by the Certificate Authority

The merchant can now add these details on his webpage to enable the prospective customers view the product. The merchant would add the product details and the certificate details and

click on save. This will then display the product. This is depicted in the diagram below (figure 7.44)

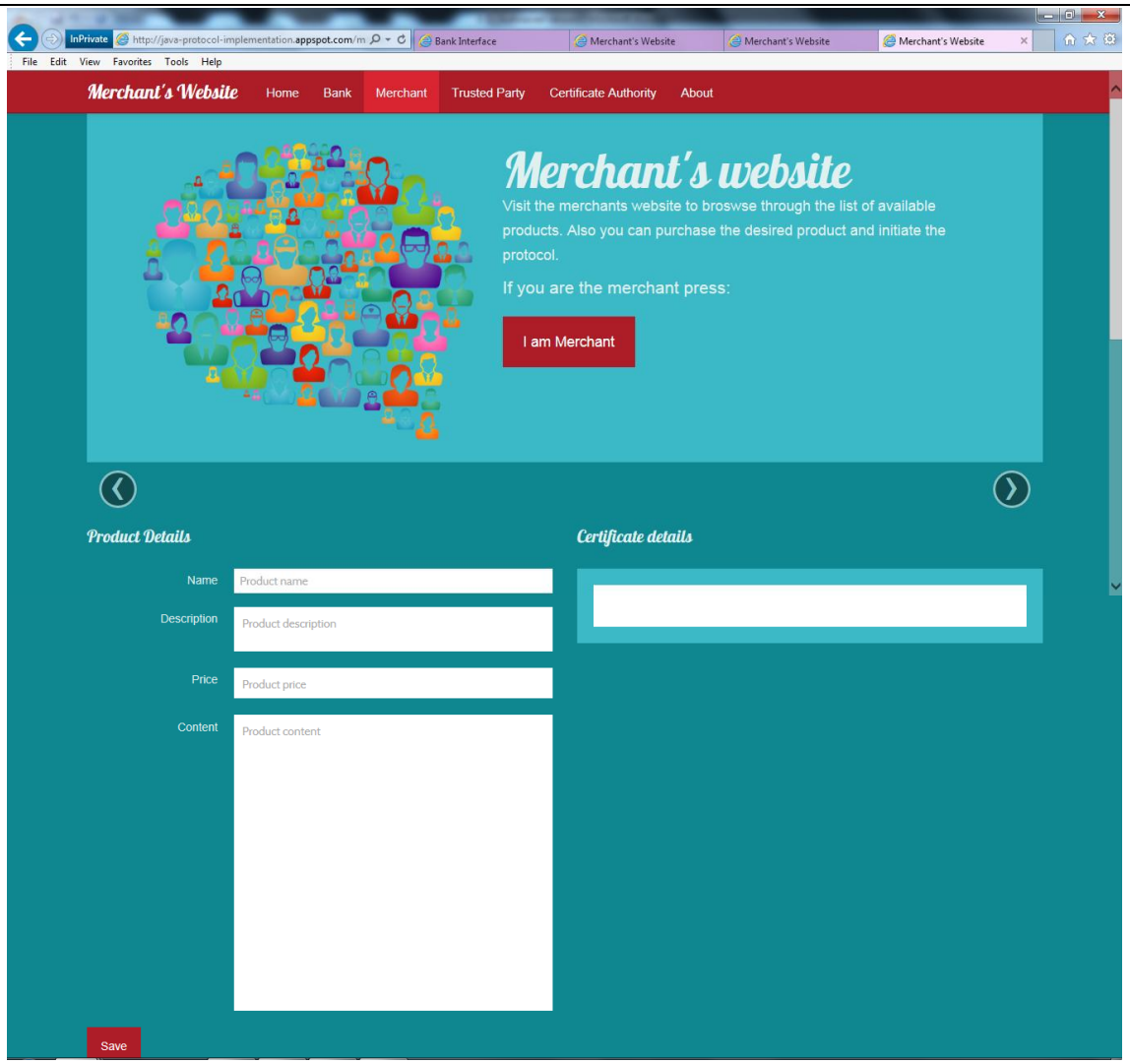


Figure 7.44: Merchant adding product on his website

7.3 Summary

This chapter has described in detail the implementation of the protocol. The prototype's features, key modules and how each module communicates with the others were also

explained. This chapter has proved that the proposed protocol is viable and that the logic of the protocol is indeed correct. It also demonstrated the fact that the proposed protocol could be implemented in real-life scenarios without much ado. This implementation has also shown that the communication and data flows of the proposed protocol work fine and that the desired outputs are obtained.

CHAPTER 8: VERIFICATION AND EVALUATION

The main aim of this chapter is to verify and evaluate the proposed "imposing Anonymity and Fairness Protocol". This chapter starts by introducing the concepts of formal verification and evaluation, and describes the various techniques that are used to verify and evaluate protocols in detail. It then discusses in detail the pros and cons of each of the verification techniques and methodologies followed. Based on the Key Process Indicators, this chapter compares the proposed "Imposing Anonymity and Fairness Protocol" against various protocols, and also provides evaluation criteria to demonstrate how well the proposed protocol fares under different scenarios.

Chapter Objectives:

- Enable the reader to understand the concept of evaluation, and to introduce the reader to the various techniques and methodologies that are in vogue. It also explains the advantages and disadvantages of using each method.
- Understand the key differences in the techniques that are used, and be able to see a comparison of how well the proposed protocol fares against similar protocols.
- To be able to see how the proposed protocol fares against various informal verification criteria, and also see how effective the informal verification process is.

8 Verification and Evaluation

The proposed protocol needs to be verified to ensure that it is not prone to errors, and that under all given circumstances it achieves the key aims and satisfies all the conditions. It is therefore required that the proposed protocol be thoroughly analysed using various methods to ensure that all granular details are addressed, and that these do not introduce any deviation to the proposed standards.

The protocol that is proposed has a set of predefined, desirable characteristics; these include anonymity and fair-exchange. Customer anonymity can be satisfied using various key cryptographic techniques and secure channels; also, the protocol does not involve the establishment of such secure communication channels. Hence, this property or characteristic cannot be formally verified and the scope of the verification is strictly limited to fair exchange.

Verification of the proposed protocol can be done in two different ways, namely:

1. Formal verification
2. Informal verification

Protocol evaluation refers to the process whereby the protocol is assessed based on how well it performs; this entails assessing the network statistics, the time taken for the protocol to complete a transaction, the total memory it needs, et cetera.

Based on the prototype design, it is easy to evaluate the protocol against these criteria. Evaluation can assist in comparing it against similar protocols and in assessing how far the proposed protocol represents an improvement or where it needs to be further improved. As evaluation is based on the language being coded, it is important to understand that there are certain limitations, such as good coding practices, usage of the correct methods for coding, programming language features, network capacity, et cetera. Hence, it cannot be taken as a foolproof method for assessing effectiveness, as it is tied to the above factors.

8.1 Formal Verification

Formal verification of the protocol helps to detect any unanticipated situation and flaws in the design and logic of the proposed protocol. It also helps to detect any errors in the flow of communication and messages in the implementation.

There are various techniques that can be used in order to formally verify a protocol; each one requires varying amounts of time, effort and cost. Similarly there are various advantages and disadvantages to using each technique. Some of the techniques that could be used are manual proofs, theorem-proving, model checking and simulation.

Manual proofs: this is one of the oldest methods, and it requires much time and effort on the part of the protocol designer or developer. As there is human intervention and everything is done manually, this method is prone to errors and there is no absolute guarantee that the result of this verification is 100% accurate.

Theorem-proving: this helps to verify the mathematical correctness of the protocol. Not all protocols are able to use this method, and even those that can use theorem-proving cannot verify the protocol in its entirety, as only the mathematical components are verified and proved to be correct.

Simulation: this involves automating the various processes and actions of the protocol using a simulation software tool. It is a common method used for authentication and cryptographic protocols (Goubault-Larrecq, 2000).

Model checking: this is yet another effective mechanism for the verification of a protocol. As with simulation, this is an automated method that makes use of automated software tools. Model checking provides a promising methodology, especially for e-commerce protocols (Anderson et al., 2006). It enables the designer and/or developer to be able to say that the proposed protocol has indeed shown that it has all the desirable characteristics that it aimed to provide.

8.1.1 Comparisons

Now that the various formal methods have been described, it is important to understand the advantages and disadvantages of each method, and to compare these in order to identify the

correct method to adopt. Adopting the most appropriate verification method is important and should be chosen carefully; it depends on the type of the protocol, the involvement of users, the relative importance of the protocol, and the availability of tools and resources. Each method has its own strengths and weaknesses, and (depending on the requirement and the criticality) one or more verification methods could be used. The table below (Table 8.17) clarifies these advantages and disadvantages (Anderson et al., 2006).

Verification Method	**Advantages**	**Disadvantages**
Theorem-Proving	1. Helps to prove program or protocol specifications in an exact manner. 2. Helps to reduce human error. 3. Helps to provide a formal and clear structure for the purposes of verification.	1. Not much documentation is available. 2. It is complex in nature and hence requires much experience and expertise. Thus, it is not easy for every individual and is not the apt choice for those that do not possess the skills. 3. No counter examples are provided in case the theorem fails.
Simulation	1. Automated and has a great deal of computational power that could be relied on. 2. Saves much human time and effort. 3. Faster than manual methods.	1. Given the nature of this method, it requires much work to be done every time the model changes, as it is ad hoc and must be remodelled each time and for even the slightest

		change. 2. Simulation allows the developer or designer to simulate only a few given scenarios. This means that not all scenarios are taken into consideration.
Manual Proof	1. Provides the developer or designer with a great deal of flexibility in deciding what needs to be done. 2. Proves to be a simple and easy-to-use method if the protocol is straightforward. 3. Very cost effective and does not require any computational power or tools.	1. It requires a lot of effort and is very time consuming. 2. Given that there is human involvement, the chances of error are high. 3. It has limited capability and can become very difficult in the case of a really complex problem. 4. It could become difficult for any individual to take into account all scenarios, and hence might not provide a complete result.
Model checking	1. It is fast, robust and provides a more effective and efficient solution. 2. Given the nature of	1. In the case of business modelling, this might not be the most viable solution. 2. Given that it is

	the model-checkers, it is easy to identify the exact point of failure, and it also provides counter examples. 3. Identify the critical points of failure or the pivotal flaws relating to flow of information that other techniques fail to identify.	language specific, the expressiveness is limited to the language and is subject to the constraints of the language in which the protocol is modelled. 3. This might mean that the entire protocol itself might not be thoroughly validated. It just enables certain aspects of the protocol to be validated.

Table 8.17: Verification methods advantages and disadvantages

8.2 Informal Verification

The informal verification methods and technologies were commonly used earlier. This method involves listing the scenarios that could occur, and possible attacks or areas that could go wrong are determined. For security protocols, however, informal methods are not very effective. This is because it becomes very difficult or nearly impossible to be able to determine all modes of attack and threats that might occur (given that there are new threats and system vulnerabilities that are discovered every day, and also given the vastness of these). It is ad hoc by nature – this means that there is no specific rule on how scenarios are listed or what scenarios are taken into consideration. Given that there is no scientific way of approaching this, there is also no guarantee that all scenarios are taken into account (Kong et al., 2000).

Some researchers (e.g. Wang et al., 2001) describe how ineffective this method is. They suggest that e-commerce protocols involving security and cryptographic mechanisms need a stronger

form of verification due to the complex nature of these protocols and the errors that could be caused due to human intervention. They describe how it is important for all the stakeholders of the protocol to be involved in all the stages of verification in order to ensure that various attack scenarios are addressed and to ensure that the protocol is fail-safe and resilient.

This research used two different methods to verify and evaluate the protocol. Firstly, the logic of the protocol was evaluated by implementing a prototype. This evaluation helped prove that the protocol's logic was indeed correct and that the protocol could be used as a viable solution in the real-world. The implementation was then run using the model-checker, which helped to evaluate the network statistics and the time taken for the protocol to process the information end-to-end.

The protocol logic is interpreted by the model-checker as a transition diagram made up of nodes and internodes. A count of the number of nodes or states is made by the checker as it moves through the logic diagram to check for any assertion violations.

In addition, the model-checker also verifies the logic, that is, it assures that the software satisfies all the expected requirements. The dynamic verification of the program by the model-checker is helpful in diagnosing for bugs in the program. These bugs could sometimes not be revealed while working on the implementation of the prototype. The model-checker helps to trap even those that could be ignored during development.

As a whole, the program is verified and the results are supplied through logical evaluation. In our case, we have found unhandled exceptions about array indices out of range; however, this can be further verified by compiling the program logic pack as a project/solution and resolving the exception by checking for any array indices to be resized.

To check this, the implementation that was originally done using Java was recompiled, as the converted C# code might have the issue of resizing the relevant array index size to meet the logic requirements. On doing this, it was found that the original Java code compiled properly without problems, and hence this issue can be closed as the modelling is, by itself, successful.

The following table (Table 8.18) 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

Table 8.18: Program execution time

The table below (Table 8.19) 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	Time
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

Table 8.19: Memory usage for each executable file

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

The research goal of developing a protocol that is both effective and efficient is satisfied by the above two evaluations of time and memory. The speed at which the protocol is being run plays a critical role in determining the effectiveness and efficiency of the protocol. As the application of the protocol would be one of the key factors in determining the success or failure of a business, time plays a major role. A protocol that takes a lot of time to implement would not be a

favoured choice by either the business or the end-user or customer. A shorter execution time would mean that the total turnaround time for the transaction would be less and would also result in a significant reduction in waiting time.

Another way to discuss the effectiveness of the protocol is to compare it with similar protocols - that is those protocols that have the same characteristics and properties. This helps identify how well the proposed protocol performs and how well it helps manage the research gaps identified. The protocols are compared against the key performance indicators. These key performance indicators include:

1. Number of messages sent
2. Type and role of the Trusted Third Party (TTP)
3. E-commerce phases covered
4. Dispute resolution mechanism in place
5. Fairness in all stages
6. Complete anonymity

The proposed protocol is compared against the following protocols:

Ray: An anonymous and failure resilient fair exchange e-commerce protocol. This protocol has a total of 10 messages that are exchanged between all the parties.

Zhang: A mutual authentication enabled fair exchange and anonymous e-payment protocol. This protocol uses many rounds of authentication in order to achieve fair exchange and anonymity. Hence, too many messages are and received. The entire protocol has six different phases.

Key Performance Indicator	**Imposing Fairness Protocol**	**Ray's Protocol: An anonymous and failure resilient fair exchange e-commerce protocol**	**Zhang: A mutual authentication enabled fair exchange and anonymous e-payment protocol**

Number of messages sent	7 messages	10 messages	11 messages and 6 phases
Type and role of TTP	Paritally Trusted online third party but controls in place to circumvent TTP to modify or read messages	Semi-trusted Online Third Party	Semi-trusted Online Third Party
E-commerce phases covered	All phases. The protocol addresses all phases of e-commerce from pre-negotiation to the delivery phase.	Does not include the pre-negotiation phase and the protocol assumes that this would be taken care of.	No provision for providing fair exchange during the negotiation phase and does not discuss the issue of withdrawal (what happens if either of the parties decide to withdraw from the transaction).
Dispute resolution mechanism in place	Inbuilt mechanism for dispute resolution. Also the Trusted Third Party stores information in case of disputes arising post-delivery of goods.	It assumes that the parties to not misbehave and does not discuss dispute resolution mechanism when either or both parties misbehave.	Does not discuss what happens when both the parties are dishonest and that part of the dispute resolution is not specified.
Fairness in all stages	Yes	No – if the Trusted Third Party is dishonest then fairness is not achieved.	No – not provided during the pre-negotiation phase.
Complete anonymity achieved	Yes	Yes but becomes a bottleneck due to the large number of pseudo-identifiers created.	Only partial anonymity is achieved.

Table 8.20: Protocol comparison using key performance indicators

From the performance indicator table, it is clear that the Imposing Fairness Protocol fares much better when compared with the other two protocols in all the key performance indicators mentioned.

8.3 Model checking

Model checking has become very popular in recent years and is an evolving field. It offers a platform to verify and evaluate protocols in an effective and efficient manner. It is a formalised evaluation and verification process. Model checking is thus a mechanised technique which could be used to discover scenarios that could lead to failures and specifically to showcase those areas of concern whereby design changes need to be considered.

Model-checkers have a few key tasks to perform. These tasks are as follows:

1. Specification of the model. This refers to a process whereby the system is defined clearly.
2. System requirement specification and definition. The system requirements are those properties that need to be tested.
3. Verification and checking. The model-checker checks the properties defined to see whether or not these hold good; it also checks for system behaviours.
4. Provision of counter examples. This is the fourth pivotal task performed by the model-checker, and one of the main advantages of using model checking over other techniques. When the model-checker finds out that the system behaviour or the properties specified do not hold good, it proposes counter examples and also explains why those properties failed.
5. Some model-checkers have the ability to provide random simulation of the system to further enhance the verification. (Clarke et al., 1999)

Many model-checkers are available and many of these have different capabilities, and so choices are based on requirements. Researchers make use of various model-checkers to ensure that the protocols proposed are verified thoroughly. The most popular of these model-checkers are as follows:

- FDR – Failures Divergences Refinement: more of a refinement-checker rather than a typical model-checker, these software tools are designed to check formal models that are expressed in Communicating Sequential Processes (CSP). This was designed and developed by Formal Systems Ltd. (Formal Systems Ltd., 2013).
- VeriSoft - Designed by VeriSoft: this model-checker is used for exploring the state-space of an implementation and is based on the C programming language. This is particularly

useful for concurrent systems, i.e. systems that are composed of many processes or elements that run concurrently (simultaneously) and have the ability to communicate with each other (P Godefroid, 1997).

- SPIN – developed by Holzmann at Bell Labs: this has a simulation feature available that can be used to simulate different scenarios. This model-checker checks for the code written in PROMELA (Process Meta Language), which is very similar to the C programming language (SPIN, 2013).
- MoonWalker: this is a model checker similar to VeriSoft in that is used for exploration of the state-space of a program that is written in bytecode (.NET applications). This is based on a Mono C# compiler (Aan de Brugh, 2009).
- SMV – Symbolic Model Verifier: this model-checker was developed by SMU and is one of the very first model-checkers, designed in the early 1990s. This was one of the most successful and powerful tools at that time. It provides a true or false output; true indicates that the property holds good, and false that the property does not hold good. It also gives a trace as to why it is false. (CMU, 2013).

The above is not a complete and exhaustive list of all the model-checkers available. It only gives a list of the most popular ones or those that have been used by other researchers for verifying e-commerce and security protocols. For example, Ray's protocol uses the FDR model-checker and Wang et al. makes use of both VeriSoft and SPIN for the verification of their protocol. AlAraj uses the SPIN model-checker for model checking his Enforcing Customer Honesty Protocol (A AlAraj, 2008).

8.4 MoonWalker Model checking Tool

This section describes the model checking tool that was selected and 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 is used for the formal verification of the proposed protocol is MoonWalker. MoonWalker is a software model checking 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, which is used to run the C# compiled bytecode (.NET).

The MoonWalker software tool uses an approach called 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 MoonWalker due to name clashes. The design was 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 (one that does not confuse the user). An extensive test framework, to detect most flaws in logic and flows, is also added to the most recent version.

The version that is used for the research purpose is MoonWalker 1.0. This version of the software uses a different approach, which is based on the concept of shortest-path-first. Based on this, a new algorithm called the Memonised Garbage Collector (MGC) is implemented. This detects various changes in the state of the process or activity (objects). This tracks the changes of any given object from the beginning stage to its end stage (Aan de Brugh, 2009).

The figure below (Fig 8.45) gives a conceptual overview of MoonWalker's model checking functionality. As described in the above paragraph, precompiled C# (.NET) source code, which can be executed by the .NET runtime environment, is loaded along with the assertions specified within it to the Moonwalker model-checker tool. This precompiled executable C# code is also known as a .NET assembly. The tool explores the state-space of the assembly. The state-space is a space whose axes are the state variables. The state-space representation is a mathematical model of an actual system (in this case the software) as a set of input, output and state variables, related by equations. In simple terms, the .NET assembly file and the assertions (true or false statements) that need to be tested or checked against are fed into the MoonWalker tool. The tool then analyses and displays the results. A result could either be a pass, which is OK,

or it shows the assertion violations. The place where the assertions are violated are also specified.

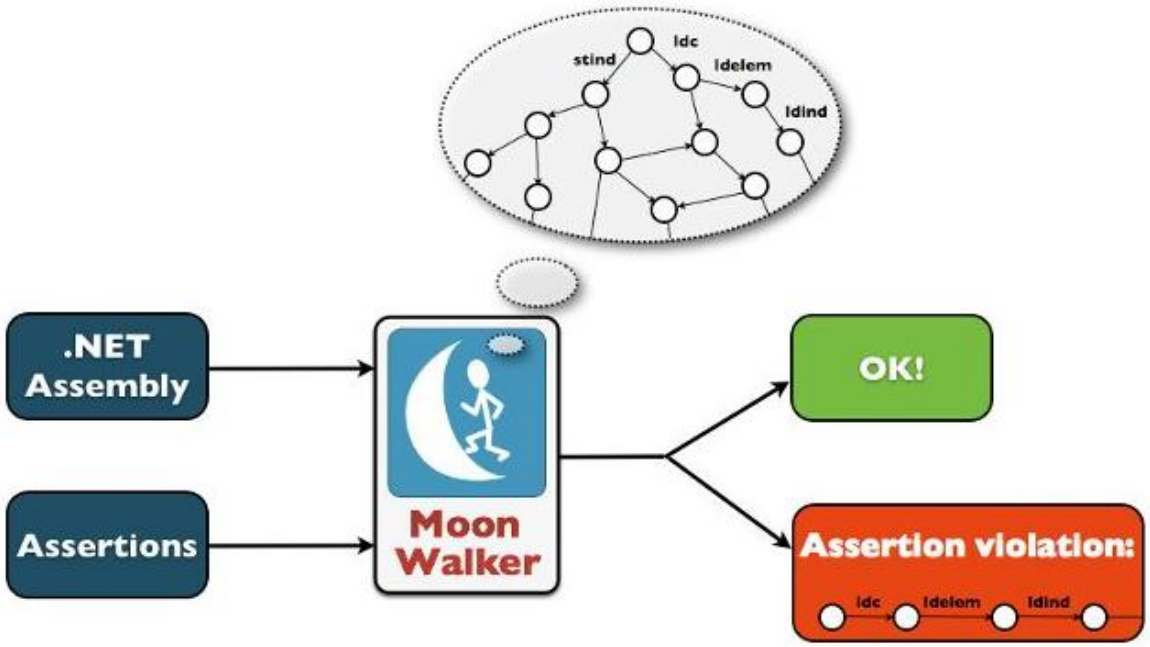


Figure 8.45: Conceptual view of the MoonWalker model checking tool

Figure source: www.simple-talk.com

8.4.1 The process

As discussed in the previous chapter, the protocol's prototype was written using the Java programming language. This source code (written in Java) was rewritten in C# language. The re-written code was then compiled using Visual Studio 2010 Professional. The purpose of using C# was to ensure that the compiled code could be used with the MoonWalker tool (to be able to check for assertion violations and deadlocks as well as race conditions). Mono C# compiler, which is based on Command Line Interface (CLI), was used primarily in order to be able to run the MoonWalker tool and to model the protocol's prototype.

The main aim of the modelling was to help identify the following key issues, and to determine that the protocol was free from the same. These are:

1. **Assertion Violations:** an assertion is nothing but a true/false statement (known as a predicate). It is a statement that the developer always assumes to be true. So while model checking, if false is obtained at run-time, then this results in an assertion violation. For example, the protocol always assumes that the encryption would be successful and that there would be no loopholes. When this assertion is run through the model-checker, this must return true. A false value represents a flaw in the assumption, thus leading to an assertion violation. An assertion in general is used to indicate the validity of certain modules and also to check for the program's correctness. Assertions in certain cases are also added to help with error-handling.
2. **Deadlocks:** a deadlock situation occurs where two or more competing actions are waiting for each other to execute, where neither ever does. For example, say there are three actions A, B and C. A cannot carry out a transaction until it has input from B. In order to provide that input B has to wait for C to finish but C is waiting for an instruction from A to be able to finish. Here all the three processes are held indefinitely as these are waiting for each other to be able to continue execution. This leads to a stage where the program will not be able to continue. It is a problem when there are many processes involved in a program.
3. **Race Conditions:** this refers to a situation when the program or application module can be executed correctly only when the sequence of threads or processes run in a specific order or timing. Race condition can lead to unexpected behaviour if it is not critical or in certain critical cases can lead to bugs or invalid execution of the program or application module. To illustrate this let us assume that there is a global variable GV. Two different modules, namely A and B, would need to read the value of this variable and increment it by one. But the condition is that it has to be mutually exclusive (this means that the operation of reading and writing cannot be interrupted).

Normal execution of the program or code is shown in the table below (Table 8.21).

A	B	Value of GV
Read		0
Increment		1
	Read	1
	Increment	2

Table 8.21: Normal execution of the program or code

The table below (Table 8.22) shows what happens to the flow when there is an interruption:

A	B	Value of GV
Read		0
	Read	0
Increment		1
	Increment	1

Table 8.22: Interrupted flow, which leads to race condition

As incrementing happens simultaneously, and A and B are not mutually exclusive; this results in a race condition whereby the value of GV gets updated only once, thus leading to an incorrect output.

Given that the original prototype was written using Java, certain modifications had to be made as they were inevitable in ensuring that the C# programs compiled successfully into executable files. Care was taken to ensure that wherever possible, the source code programs were seen as units and where necessary (keeping in mind the output required), the source code programs were seen as one whole project on Visual Studio. For example, to identify the time taken by individual modules (e.g. encryption), the necessary program was taken as a separate unit and compiled, and when the execution time for the whole protocol was required, all programs were compiled together as a project.

During the model-check, in the case of no assertion violations being found, OK is outputted. Otherwise, a trace of instructions that leads to the assertion violation is generated, which can be an output to a file for reading. The instructions are given in CIL or Common Intermediate Language, which is used by the Microsoft .NET framework and the Mono compiler that has been

used for this exercise. MoonWalker is a CIL assembly that is developed on Windows XP, and Mono and works on this platform.

8.4.2 Model Checking - Analysis

The MoonWalker model-checker has two panes. The right pane has the solution explorer and the left pane lists all the program references. These programs are written in the C# programming language and have the .cs extension.

The source code programs are given on the right-hand side on the solution explorer. This is the equivalent of the Java program that was written for the purposes of implementation. Many individual programs were compiled together to be run and packaged together as one individual executable project. This was done in order to ensure that the entire project (or the executable) was modelled and not just the individual modules. The key programs compiled into one project as “compile.exe” are as follows:

- EmfInstanceManager.cs
- EncryptionHelper.cs
- TrustedTransaction.cs
- MerchantApi
- EntityManager.cs
- Order.cs
- Payment.cs and
- Product.cs.

Once the above mentioned files were bundled together and the compile.exe file produced as a result of the compiled project, this was fed into the model checking tool MoonWalker.

Output with statistics turned on were run in order to understand and analyse if there were any assertion violations or deadlocks. The statistics also showed the amount of memory space each module occupied along with the time taken for the module to execute. While compiling the program there was one exception that was encountered.

The output here enables us to identify the deadlocks, race conditions and assertion violations. MoonWalker enables the user to output with the statistics feature turned on. All outputs would be displayed in a separate console (similar to a DOS-based console). The statistics feature shows any memory error or management issues, bug management issues, et cetera. It also allows the user to select which features need to be enabled and those features that need to be set to false or disabled. For example, in the figure below, the properties StoponError and TraceonError are set to true or, in other words, enabled. This means that the MoonwWalker tool would halt an execution when a bug is found and would display the same. Similarly, the TraceonError feature would allow the user to trace the error in a step by step fashion that would enable the user see the intermediate result of each and every line of the code, and to identify the root cause of the bug by placing check points.

Thus, the output of the model-checker can be interpreted in a straightforward and consistent fashion by studying the console statements displayed. The first few statements show that features such as Statistics are enabled in the configuration, whereas features such as the "Interactive" mode are set to false. This was displayed by running the compiled executable file, compile.exe using the argument '-s', such as: compile.exe –s. Arguments in MoonWalker are very similar to Linux-type commands. These arguments tell the MoonWalker tool what exactly is required and what needs to be done. Arguments have the prefix '–' (hyphen) followed by an alphabet letter or a word. Two or more arguments can be combined together by following one hyphen, which is again very similar to the Linux-based environment.

First, all the programs were complied together as one single unit. Key points derived from the output of the model checking are as follows:

- An exception has been encountered. This is the System.IndexOutofRange exception.

  For the runs of all programs through the model-checker, an unhandled exception has been encountered during the model checking towards the end, as a System.IndexOutofRange exception. Although this message does not indicate deadlock or race condition explicitly, it may need to be revisited to ensure that there is no issue. Moreover, it is important to note that exceptions are issues relating to compilation and program structure. The model-checker checks for assertion violations and reports on

conflicts such as deadlocks or infinite loops, i.e., it reports on the modelling behaviour of the program logic.

This exception might have occurred due to the fact that the code was originally written for Java and then rewritten in C# for the purposes of model checking. As the Java code did not show any exception, this could be taken as an issue that has occurred only because of the conversion in the language and is nothing serious.

Once it was clear that there is no major problem with the program compiled as a whole, the individual modules were then run through the model checker. The outputs and screenshots are attached in the appendix of this thesis.

8.5 Summary

This chapter has discussed in detail the evaluation and verification of the protocol. It discussed the different verification methods that are available, and compared the various methods to point out the advantages and disadvantages of each. Furthermore, it provided a clear description of the evaluation methods and presented statistics on how well the proposed protocol performed. It finally compared the various protocols to show how effective and efficient the proposed protocol is, when compared with the other protocols.

This chapter has explained the basics of model checking and described in detail the model checking tool MoonWalker. It also discussed the output of the model checking in detail and from the results of the model checking done on the compiled project (as well as on the individual files of the program), it may be concluded that the logic of the protocol holds good and that the project has passed the modelling test. Apart from unhandled exception and the ArrayIndexOutofBounds exception, no other issues were encountered. It is important to note that these do not signify any errors or flaws in the logic (or in the model itself; rather, it just shows that there could be issues with the build (which is a programming issue). It should also be noted that these issues could have occurred due to the programming language change from Java to C#. Hence it can be stated that the model satisfies the fair exchange property.

While it is clear that the modelling has been a success, it is key to understand that the protocol's model and the actual protocol itself might be two different things. This is because the model cannot in its entirety represent the logic of the protocol, and also that it is only an abstract way of representing the protocol. The idea of modelling the protocol is not to drill down to the detailed level of all attributes of the protocol, but to check the protocol against certain specified behaviours that it might exhibit, to be able to verify it and to see if it holds good. From the above, it can be shown that the protocol clearly fares well by satisfying the key properties mentioned, and behaves in an appropriate manner, as required.

CHAPTER 9: CONCLUSION

The main goal of this final chapter is summarise all the other chapters and also to give a brief explanation of how the aforementioned objectives of this research have been successfully achieved. It also helps to measure the level of success of this research.

Chapter Objectives:

- Enable the reader to understand the protocol's achievements
- Provide an overview of the other protocols that formed the basis of the research, and to quickly recap the disadvantages of those protocols.
- Understand the various methods that have been used to successfully achieve the objectives of the research.
- Highlight the various methods that have been used to verify and evaluate the proposed protocol.

9 Conclusion

The research primarily was concentrated on two key aspects of an electronic commerce protocol, namely fair exchange and anonymity. It concentrated on these as they help to increase trust in e-commerce websites. Various studies (Anon, 2001; Forrester, 2001; Westin, 1991; Westin, 1994) have pointed out that many of the customers who use e-commerce are still sceptical, and that the e-commerce market has an even greater potential if one aspect is adequately addressed: trust. These studies also point out that customers would be more willing to engage in e-commerce (and potential new customers would also be attracted) if they could be assured of privacy. This was proved in a recent report by Gartner (Gartner, 2005), which clearly shows that customer privacy is not fully respected in e-commerce, and that this trend may increase, which would result in people eschewing such technologies, thereby limiting their growth.

From this research, it has been clearly demonstrated that trust plays a major role in e-commerce and that it can be perceived from many different angles, namely technological, psychological, legal, business, etc. The technological aspect of trust has been addressed in this research to a certain extent by ensuring that the building blocks of technology (the basic protocol that is used for electronic commerce) deliver fair exchange and that the identity of the customer is protected. Fair exchange gives both the customer and the merchant the confidence to know that they will not be cheated in the end. This increases trust. Similarly, the customer's uncertainty over whether their personal information will be misused (e.g. identity theft while shopping online) is addressed through anonymity, whereby the customer's identity is kept secret and the merchant or any interceptor will not be able to trace back the transactions to the customer. One research (R Smith & J Shao, 2007) shows that customer privacy plays a major role in increasing trust in e-commerce, and that it is beneficial to both customers and e-business. From a customer point of view, personal choices are kept secret and transactions untraceable, hence increasing trust and satisfaction. From a business point of view, increased customer satisfaction leads to more business and greater revenues. Enabling privacy by making use of anonymising technologies is thus an attempt at creating an acceptable level of trust in e-commerce.

The research identified four protocols (Ray, 2005; Zhang, 2006; Zhang, 2003;Franklin & Reiter, 1997) that concentrate on both anonymity and fair exchange. Thorough review of literature enabled identification of the drawbacks of these protocols. The research then aimed at developing a protocol that would counter these drawbacks and provide not only anonymity and fair exchange but also payment security. The protocol made use of an online Trusted Third Party (TTP) and provided fair exchange throughout all phases of the electronic commerce transaction, namely the pre-negotiation, negotiation, withdrawal, purchase and arbitration phases. The protocol was also designed in such a way that it provides automated dispute resolution. The designed protocol was made efficient by ensuring that the number of messages was kept to a minimum. Automated dispute resolution ensures that the TTP would be able to provide time-stamped and accurate data when required.

It is also important to note that the protocol takes into consideration that either of the transacting parties, namely the customer or the merchant, can at any time withdraw from the transaction. If either or both the parties wish to withdraw at any point in time, the protocol can be terminated. The protocol also assumes that one or more parties can be dishonest and is therefore capable of terminating the transaction when dishonesty on the part of one or more parties is discovered. For the protocol to continue with the normal flow, the transacting parties are required to remain honest, and fairness in any transaction is then imposed by the protocol.

This research identified the key drawbacks in the other protocols that provide both anonymity and fair exchange. These include one or more of the following:

- A TTP that was not entirely trustworthy (semi-trusted).
- The protocol(s) was complicated with many rounds and too many messages.
- The protocol had not taken into account what would happen if more than one party was dishonest.
- The protocol did not provide complete anonymity.
- The protocol did not provide fair exchange across all stages of the e-commerce transaction.

The proposed protocol has significant advantages. These are:

- The TTP's semi-trusted nature is taken into account and controls are placed to make sure that this partially trusted attribute of the TTP is circumvented. The TTP cannot masquerade or join another party to conspire against the remaining party. The protocol also ensures that the TTP cannot modify any messages that are being sent. This additional security makes the TTP completely trustworthy.
- The protocol is simple to use and with a limited number of messages.
- The protocol takes into account that more than one party can always be dishonest and terminates when it detects dishonesty.
- It provides complete anonymity for the customer across all phases.
- It provides fair exchange throughout the e-commerce transaction.
- In addition to anonymity and fair exchange, the protocol provides payment security by ensuring that the payment tokens cannot be duplicated or reused by either of the transacting parties.
- It makes use of symmetric key cryptography where possible. This ensures that the protocol is kept simple and offers better performance.
- The protocol offers automated dispute resolution. In simple terms, it has a built-in dispute resolution mechanism. The TTP can be able to give accurate data regarding transactions, as all messages are time-stamped and stored.
- The protocol makes use of a single payment token. This means that whatever the cost of the digital product, only one payment token is used per transaction. In simple terms, this means that the denomination of the payment token is variable and is dependent on the amount that is required. In the proposed protocol, cash withdrawal is done only once during the entire e-commerce transaction as only one payment token is required. This makes the protocol less cumbersome and increases effectiveness.
- The protocol offers security by means of hashing, encrypting and time-stamping the messages. The time-stamping ensures that replay attacks are avoided (even if intercepted by someone in the middle).
- Using both asymmetric and symmetric key cryptography ensures that neither participant is required to store and distribute many keys. Asymmetric key cryptography is used only when absolutely necessary, thus avoiding issues relating to key management.

To test the efficiency of the proposed protocol, it has been subject to scrutiny under different circumstances. The protocol has been evaluated and verified using both formal and informal verification methods. The simulation of the protocol was conducted using Java and this ensured that the protocol is ready to use; the output of the protocol was also verified. This also proved that the protocol could be adapted to real-world scenarios without much ado, and that it is not just a theoretical idea that might not be of practical use. The formal verification method (using model checking) ensured that the protocol satisfies the key property of fair exchange throughout all stages of the transaction process. This was also done to highlight the fact that there have been no critical errors, assertion violations or race conditions that could lead to an abnormal termination of the protocol or lead to the protocol not being able to achieve the fairness property.

Different verification methods and techniques were used from different perspectives and with the aim that each verification method would complement the other. For example, the design of the prototype using Java was done with the point of view of implementation and testing the protocol's readiness and adaptability in the real world. This was complemented by running it through the model-checker. Model checking was done with the view point of testing the process-orientation of the proposed protocol and testing the protocol's logic and correctness. This was further complemented by conducting a scenario analysis, which was done from the point of view of checking the protocol's methodology. All those scenarios that could not be tested using the other two methods were taken into account to give a complete picture and to guarantee that the protocol has been tested to its entirety without leaving anything to chance. From the verification and evaluation that has been done, it could be said that the proposed protocol has been designed well and satisfies all the key criteria mentioned in the research objectives. It could also be said with certainty that the protocol has a huge potential in the electronic commerce arena if implemented, as it overcomes a major challenge of customer data privacy, as mentioned in the research by Gartner (Gartner, 2005).

9.1 Success Criteria & Contribution Revisited

The introduction chapter of the thesis defines the contribution of this research and the success criteria for the research. This section revisits the success criteria to evaluate the contribution of the research and to see how well the research has contributed.

- The research is deemed to be successful as the first measure of success has been achieved. The research has answered all the research questions.
- The second measure of success listed in the introduction has also been fulfilled as the research has conducted an in depth analysis to determine the difference between various other protocols and the proposed protocol to show how efficient it is. The literature review has successfully identified the key gaps in the other researches and has determined the need for the protocol. Chapters 5 - 8 has clearly analysed the protocols and shown how effective the proposed protocol is in comparison with other protocols.
- Development of the protocol: The research aimed at designing a protocol that was effective and also practical. The protocol has been developed to overcome the defects and gaps that were identified in the other protocols.
- Specifying the effectiveness criteria of the protocol: The protocol clearly defined the number of messages. It also provided an explanation of various key performance indicators and described why these KPIs were chosen to measure effectiveness.
- Automated dispute resolution: The research designed a protocol that has automated dispute resolution. The importance of having a good dispute resolution mechanism has been identified and explained.
- Protocol analysis: The proposed protocol is analysed completely in all given circumstances and scenarios. The protocol has also been put through theoretical verification by taking into account all possible scenarios for dishonesty and how these would be detected. The research has also defined the areas of dispute and which party would be responsible for initiating a dispute resolution.
- The prototype developed proves that the protocol can be adopted in real-world scenarios. Furthermore it was used to verify issues in the information flows and for any logical errors.

- Model checking and verification: The proposed and implemented protocol is model-checked and verified thoroughly to validate the logical flow of steps, and also to determine that the protocol successfully satisfies all the key criteria mentioned. In simple terms, this assists in establishing that the protocol implements fair exchange, anonymity and payment security throughout all stages. It also helps identify any deadlock situations that might prevent the protocol from running successfully.

In short, the key contributions of the research can be summarised as follows:

1. This research has successfully answered the research questions.
2. The proposed system is able to provide the key features and meet the needs of the emerging e-commerce market
3. The protocol can successfully detect dishonesty and terminate
4. The parties cannot collude or conspire.
5. Ready for real-world implementation and not just a theoretical idea.

9.2 Protocol Limitations and Future Works

This section describes in the limitations of the proposed protocol. The limitations prevailing in the current protocol can be examined by future researchers and this provides some scope for enhancement of the current protocol.

1. The protocol uses Chaum's blind signature for the provision of anonymous electronic cash. This method has some known issues, such as money laundering using anonymous electronic cash. For this to be avoided, certain alternative measures need to be put in place, such as traceability by the trustees or legal authorities and ensuring that there is a cap to the amount that a customer would be allowed to spend per day anonymously.

2. The payment scheme that is provided by the protocol is based on RSA. There are two disadvantages here: RSA has some known vulnerabilities and could be subject to attack, and the second one is that RSA is quite complex and has many computational modules that consist of several modular exponentiations. This complexity could affect the

proposed protocol's efficiency, particularly in cases where there is not much computational ability or resources at the participant's end.

Future research could include trying to overcome the limitations mentioned above. For example, various payment methods are available that are non-RSA based. These methods could be tried to see if the effectiveness of the protocol could be improved.

While working on further developments to the proposed protocol, the researcher should able keep in mind the following:

1. Complexity: making changes to the payment scheme or adapting different methods for ensuring anonymity might lead to the protocol becoming more complex with increased number of messages. The researcher should also take into consideration the execution time of the protocol and if implemented the amount of memory it takes. It should be understood that the timing, memory space and the number of messages are all directly proportional to the protocol's efficiency. Future developments to the protocol should therefore ensure that the advanced versions still have the efficiency of the current protocol.

2. Security: this protocol takes into account security features. Making use of an RSA-based payment method has several advantages too. Though RSA is subject to attack, the success rate of an RSA attack is still low. Given the popularity of the RSA-based payment method, it is imperative to understand that the RSA method has been subject to much scrutiny within the security community and is thus considered highly secure. Introducing a different payment method might lead to compromises on the security front. Therefore, future researchers should take into account the security of the protocol and should ensure that security is in no way compromised.

3. Readiness: the proposed protocol is ready for implementation and can be adapted to any real-world scenario. This has been proved by implementing the prototype of the protocol in Java. It has also been shown that the protocol can be implemented on an even more advanced platform to enable it to work on mobile devices. This is one of the key advantages of the protocol and future developers should take this into account and

make enhancements to the existing protocol in such a way that it would still remain robust and ready for the real world.

References

1. Aan de Brugh (2009) MoonWalker: Verification of .NET Programs, Tools and Algorithms for the Construction and Analysis of Systems, Lecture Notes in Computer Science AVolume 5505, 2009, pp. 170-173, Springer Link.

2. Al-Dwairi and Kamala M.A. (2010) Business-to-consumer e-commerce Web Sites: Vulnerabilities, Threats and Quality Evaluation Model, Electronics, Communications and Computer (CONIELECOMP 2010) Published by IEEE Computer Society pp. 206 -211, ISBN: 978-1-4244-5352-8, Cholula, Mexico.

3. Al-Tameem A., Zairi M., and Kamala M.A. (2009) "Critical Factors of Information Security Implementation", The Czech Republic.

4. Alaraj, A. (2008) Enforcing Honesty in E-Commerce Fair Exchange Protocols, Durham thesis, Durham University.

5. Anderson et al. (2006) Standards and verification for fair-exchange and atomicity in e-commerce transactions, Information Sciences, Vol. 176, No. 8, pp. 1045-1066.

6. Asokan et al. (1997) Optimistic protocols for fair exchange, Proceedings ofÂ the 4th ACM Conference on Computer and Communications Security.

7. Bao, F., Deng R.H and Mao W. (1998) “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.

8. Barker, E. et al. (2012) Recommendation for cryptographic key generation, NIST Special Publication 800-133.

9. Bill’s Design (2013) accessed at http://billatnapier.com/design_tips241.htm accessed on: 10/12/12

10. Boban, M. et al. (2012) The Data Quality in CRM Systems: Strategy and Privacy, accessed at http://bib.irb.hr/datoteka/514103.285-883-1-PB1.pdf

11. BS ISO/IEC 27002: 2005 (2007) Information technology - Security techniques , Information security management systems ; Code of practice for information security management (BS ISO/IEC 27002:2005 incorporating corrigendum no. 1). London, England: British Standards Institute.

12. Business Dictionary, accessed at: http://www.businessdictionary.com/definition/electronic-commerce-E-commerce.html accessed on 11/12/12

13. Calder, A. (2006) A Business Guide to Information Security, Kogan Page Publishers.

14. Chaisson, M. et al. (2011) Researching the future in Information Systems, Springer.

15. Chaum, D. (1983) Blind Signature for Untraceable Payment, Proceedings of Eurorcrypt 82, pp. 199-203, Plenum Press, New York, 1983.

16. Chaum, D. et al. (1990) Untraceable Electronic Cash, Springer-Verlag Berlin Heidelberg.

17. Clarke, R. (2000) E-commerce Definitions, Roger Clarke, © Xamax Consultancy Pty Ltd, 1997-2000.

18. Clarke et al. (1999) Model Checking, MIT Press.

19. CMU (2013) Webpage accessed at www.cs.cmu.edu/_ modelcheck/smv.html accessed on 16/10/13

20. Columbus, L. (1999) Administrator's Guide to E-commerce, LWC Research.

21. Computer Systems Laboratory Bulletin (1994)Â Threats to Computer Systems: An Overview.

22. Conceptual Model of MoonWalker Model Checker (2013) Figure accessed at www.simple-talk.com accessed on 16/10/13

23. Crnkovic, GD (2010) Constructive research and info-computational knowledge generation, Model-Based Reasoning in Science and Technology, 2010 - Springer

24. Cruz, R.T. (2003) Possible Anticompetitive Barriers to E-commerce, A report from the staff of the Federal Trade Commission.

25. Cyber Dialogue (2001) Cyber dialogue survey reveals lost revenue for retailers due to widespread consumer privacy concerns. Accessed at http://www.cyberdialogue.com/news/releases/2001/11-07-uco-retail.html accessed on 21/02/13

26. Dwairi R.M. and Kamala M.A. (2009) An Integrated Trust Model for Business-to-Consumer (B2C) E-Commerce: Integrating Trust with the Technology Acceptance Model, CYBERWORLD 2009, Published by IEEE computer society, Bradford, U.K.

27. Ford, W. et al (2000) Secure E-commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice Hall.

28. Formal Systems Ltd (2013) Webpage accessed at http://www.fsel.com/index.html accessed on 26/05/13

29. Forrester Research (2001) Privacy concerns cost e-commerce $15 billion (September). http://www.forrester.com/ accessed on 14/04/13

30. Franklin and Reiter (1997) Fair Exchange with a Semi-trusted Third Party. In T. Matsumoto, editor, Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 6, Zurich, Switzerland, April 1997.

31. Fredriksson, T. (2013) Workshop on E-Commerce, Development and SMEs, WTO, Geneva, Switzerland.

32. Gartner Research (2005) Increased phishing and online attacks cause dip in consumer confidence (June). http://www.gartner.com/ accessed on 14/04/13

33. Gefen, D (2000): E-commerce: the role of familiarity and trust Volume 28, Issue 6, December 2000, Pages 725–737, Science Direct

34. Godefroid, P. (1997) Model Checking for Programming Languages using VeriSoft, Proceedings of the 24th ACM Symposium on Principles of Programming Languages, Paris

35. Gosh, A.K. (1998) E-commerce Security Weak Links, Best Defenses, Protecting your system from vulnerabilities in browsers, servers, secure protocols and firewalls, John Wiley and Sons.

36. Goubault-Larrecq (2000) A Method for Automatic Cryptographic Protocol Verification, Springer Link.

37. Grau, J. (2006) Online privacy and security: the fear factor, available at: http://www.emarketer.com/report.aspx?code=privacy_retail_apr06 accessed on 13/05/13.

38. Harris, S. (2010) CISSP All-in-one Exam Guide, 6th Edition, McGraw Hill Publication.

39. Hassler, V. (2000) Security Fundamentals for E-commerce, Artech House Inc.

40. Head, M. and Hassanein, K. (2002) Trust in e-commerce: Evaluating the Impact of Third-Party Seals, Quarterly Journal of E-commerce, 3(3), 307-325.

41. Hines, M. (2002) Protect Privacy or Jeopardize CRM, accessed at: http://searchcrm.techtarget.com/news/843537/Protect-privacy-or-jeopardize-CRM accessed on 28/02/13

42. Hoque, F. (2000) e-Enterprise Business models and Architecture, Cambridge University Press.

43. Hsieh, C. (2001) E-commerce Payment Systems: Critical Issues and Management Strategies, Human Systems Management, Vol. 20(2).

44. Hubbard, D. (2009) The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46.

45. ICO (2013) Security Breach Notification: the ICO Point of view, accessed at http://www.ico.org.uk/news/events/previous_events/~/media/documents/library/Corporate/Research_and_reports/ico-presentation-20130919-Security-breach-notification-Jonathan-Bamford.pdf accessed on 26/08/13

46. Jannadia, O, Sadi A , Bubshait AA and Naji A (2000) “Contractual methods for dispute avoidance and resolution (DAR)” Volume 18, Issue 1, February 2000, Pages 41–49 International Journal of Project Management, Elsevier

47. Javvin (2013) Network Dictionary, accessed at www.networkdictionary.com accessed on 14/01/14

48. Kamoun, F. et al. (2012) User Interface Design and E-commerce Security Perception: An Empirical Study, University of Dubai.

49. Katsh et al. (2001) Online Dispute Resolution: Resolving Conflicts in Cyberspace, Jossey-Bass Publication (Wiley & Sons).

50. Kessler, G.C. (2013) An Overview of Cryptography, accessed at http://www.garykessler.net/library/crypto.html accessed on 20/01/14

51. Khill, I., J. Kim, I. Han and J. Ryou (2001) “Multi-party fair exchange protocol using ring architecture model”, Computers and Security, Vol. 20, No. 5, pp. 422-439, USA.

52. Kimpl (2012) Accessed at http://www.kimpl.com/920/anonymity-privacy/ accessed on 11/11/13

53. Kong et al. (2000) Formal analysis of an anonymous fair exchange e-commerce protocol, Proceedings of the 4th International Conference on Computer and Information Technology, pp. 1100-1107, Wuhan, China.

54. Kong et al. (2004) Formal Analysis of an anonymous, fair exchange e-commerce protocol, IEEE Symposium.

55. Kono, T. et al. (2002) Selected Legal Issues of E-commerce, Kluwer Law International.

56. Kremer, S. et al. (2002) An intensive survey of fair non-repudiation protocols, Comput. Commun., Vol. 25, pp. 1606-1621.

57. Li et al. (2003) A Reputation-based Trust Model for Peer-to-Peer E-commerce Communities, Proceedings of the IEEE International Conference on E-commerce (CE03).

58. Lin et al. (2006) Fair transaction protocols based on electronic cash, Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 383-388, Taipei, Taiwan.

59. Mann, C.L. et al. (2000) Global E-commerce: A policy primer, Peterson Institute.

60. Miller, M. (2011) The PayPal Official Insider Guide to Growing Your Business: Make Money the Easy Way, PayPal Press.

61. Min, S and Wolfinbarger, M (2005): Market share, profit margin, and marketing efficiency of early movers, bricks and clicks, and specialists in e-commerce Volume 58, Issue 8, August 2005, Pages 1030–1039, Journal of Business Research

62. New Media Trend Watch (2013) Ecommerce accessed at: http://www.newmediatrendwatch.com/markets-by-country/18-uk/150-ecommerce accessed on 11/11/13

63. NIST (2013) Digital Signature Standard (DSS), National Institute of Standards and Technology Gaithersburg, Issued July 2013

64. O' Mahony, D. et al. (2001) Electronic payment systems for e-commerce, 2nd Edition, Artech House Inc. Carbonell, M., May 2008: Secure e-payment protocol with new involved entities.

65. Oracle, 2014: Oracle Java Guide, accessed at: http://docs.oracle.com/cd/E19199-01/817-5085/concepts.html accessed on 02/10/14

66. Palmer, J.W. et al (2006) The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements, Journal of Computer-Mediated Communication, Volume 5, Issue 3.

67. Panko R., (2004) "Corporate Computer & Network Security", Prentice Hall, UK

68. Patil, Harish, Divekar, Rajiv (2014): Inventory Management Challenges for B2C E-commerce Retailers, Volume 11, 2014, Pages 561–571, Science DirectPatil et al

69. Prakash G, Ved & Shilpa S (2007) “The Empowered Payment Gateway” Computer Society of India.

70. Prins, C. (2002) Trust in e-commerce - The role of trust from a legal, an organizational and a technical point of view, Kluver Law International.

71. Qin, Z. (2009) Introduction to e-commerce, Tsinghua University Press

72. Raghuwanshi, S. (2009) A new protocol model for verification of payment order information integrity in online E payment system, Department of Computer Science, MANIT, Bhopal, India.

73. Ray, I. and I. Ray (2002) “Fair Exchange in E-commerce”, ACM SIGecom Exchange,UK

74. Ray, I., I. Ray and Natarajan N(2005) “An anonymous and failure resilient fair-exchange e-commerce protocol”, Decision Support Systems, Vol. 39, No. 3, pp. 267-292.

75. Ray, I., I. Ray and Z. Narasimhamurthi (2000) An optimistic fair-exchange e-commerce protocol with automated dispute resolution, Lecture Notes in Computer Science, Vol. 1875, pp. 84-93.

76. Rivest, Shamir and Adleman (1978) A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol. 21(2).

77. Roy et al. (2001) The Impact of Interface Usability on Trust in Web Retailers, Internet Research: Electronic Networking Applications and Policy, 11(5), 388-398.

78. Russell, R. (2001) Hack-Proofing Your E-commerce Web Site: The Only Way to Stop a Hacker is to Think Like One, Syngress Media.

79. SANS Reading Room (2012) Security for CRM Environment, accessed at http://www.sans.org/reading_room/whitepapers/application/security-crm-environment_843 accessed on 04/04/14

80. Schneider, G. (2010) E-commerce, Sengage Learning, p. 17.

81. Schneier (1996) Applied cryptography: protocols, algorithms and source code, C. Wiley

82. Skevington, P.J. and T.P. Hart (1997) Trusted third parties in e-commerce, BT Technology Journal, Volume 15, Issue 2.

83. Smith, R. and J. Shao (2007) Privacy & E-commerce: A consumer-centric point of view, Springer Science + Business Media.

84. SPIN (2013) Webpage accessed at http://spinroot.com

85. Springer Image (2010) Springer Link Images accessed at: http://link.springer.com/

86. Springer Reference (2013) Trusted Third Party definition accessed at: http://www.springerreference.com/docs/html/chapterdbid/317133.html

87. Stair, R.M. et al. (2012) Fundamentals of Information Systems, Cengage Learning.

88. Tan, M. (2004) E-Payment: The digital exchange, Singapore University Press.

89. Tang and Zheng (2007): An effective dispute resolution system for electronic consumer contracts Volume 23, Issue 1, 2007, Pages 42–52, Computer Law & Security Review, ElsevierTang

90. The EC Directive (2002) accessed at: http://www.legislation.gov.uk/uksi/2002/2013/contents/made accessed on 03/03/14

91. The SANS Institute (2008) Management 525 Project: Management and Effective Communications for Security Professionals and Managers: Quality and Risk Management. Bethesda, MD: The SANS Institute.

92. W. Wang et al. (2001) Model Checking - a rigorous and efficient tool for e-commerce internal control and assurance, Gozuita School Business, Emory University, Atlanta, Georgia, USA.

93. Wang (2005) An Abuse Free Fair Contract Signing Protocol Based on the RSA Signature, In Proceedings of the 14th International Conference of the World Wide Web.

94. Wen, X. et al. (2013) An inter-bank e-payment protocol based on quantum proxy blind signature, Quantum Information Processing, Volume 12, Issue 1.

95. Westin, A.F. (1991) Equifax-Harris consumer privacy survey. New York: Louis Harris & Associates.

96. Westin, A.F. (1994). Equifax-Harris consumer privacy survey. New York: Louis Harris & Associates.

97. Whiteley, D. (2000) E-commerce: Strategy, Technologies and Applications, McGraw Hill Publications.

98. Wooledge, G. (2011) Cryptography, accessed at: http://wooledge.org/~greg/crypto/node5.html on 08/09/13

99. Wright, D. (2002) Comparative Evaluation of Electronic Payment Systems, Infor. Journal., Vol. 40(1).

100. Xue et al. (2005) A randomized RSA-based partially blind signature scheme for electronic cash, Computers & Security, Vol. 24, No. 1, pp. 44-49

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

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

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

104. Zhang, Q., Markantonakis K. and Mayes K. (2006) 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.

105. Zhang et al. (1996) Achieving Non-Repudiation of Receipt, The computer Journal.

106. Zhang et al. (2003) An Efficient Protocol for Anonymous and Fair Exchange, Computer Networks.

107. Zhang et al. (2006) A Practical Fair Exchange E-payment protocol for anonymous purchase and physical delivery, IEEE conference on System & Application.

108. Zheng Q(2009) Introduction to E-commerce, Springer Publications

109. Zhang (2013) Concept extraction and e-commerce applications, Electronic Commerce Research and Applications, Elsevier

110. Zhou, J. and Gollman D. (1996) A fair non-repudiation protocol, Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 55-61, Oakland, California, USA.

Appendix

This section provides the screenshots that were taken during the modelling process and explains what the outputs in the screens refer to. It explains what has been tested, what the checkpoints were for every program, and how the output shows a deviation in the logic (if any).

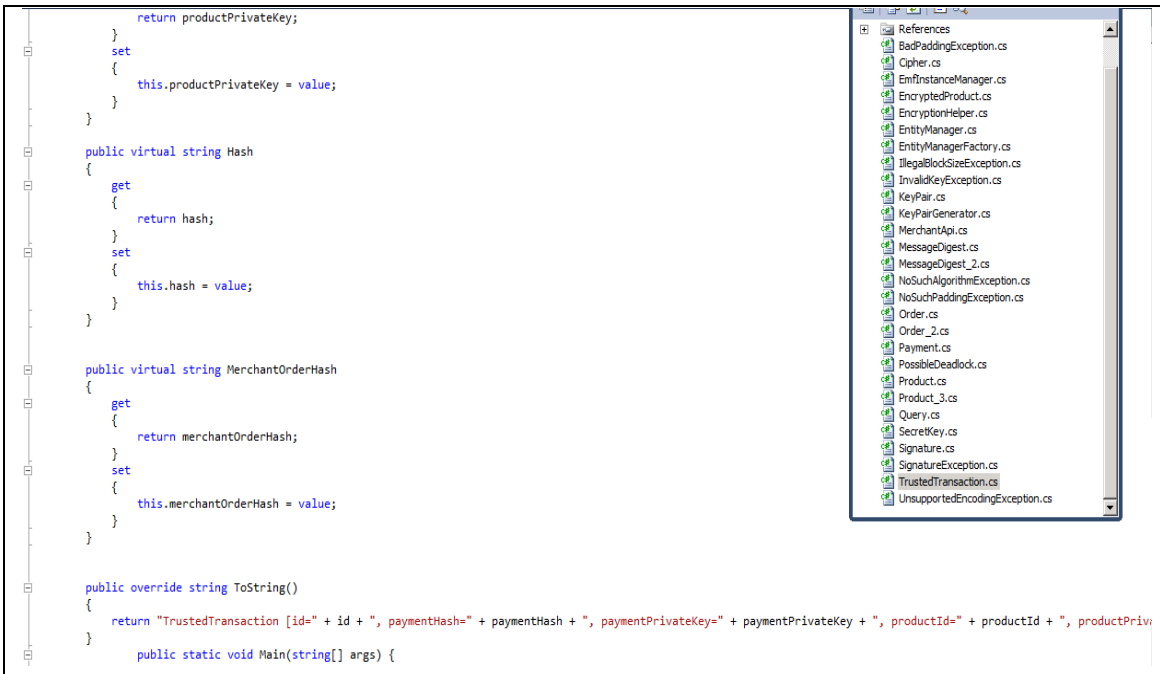
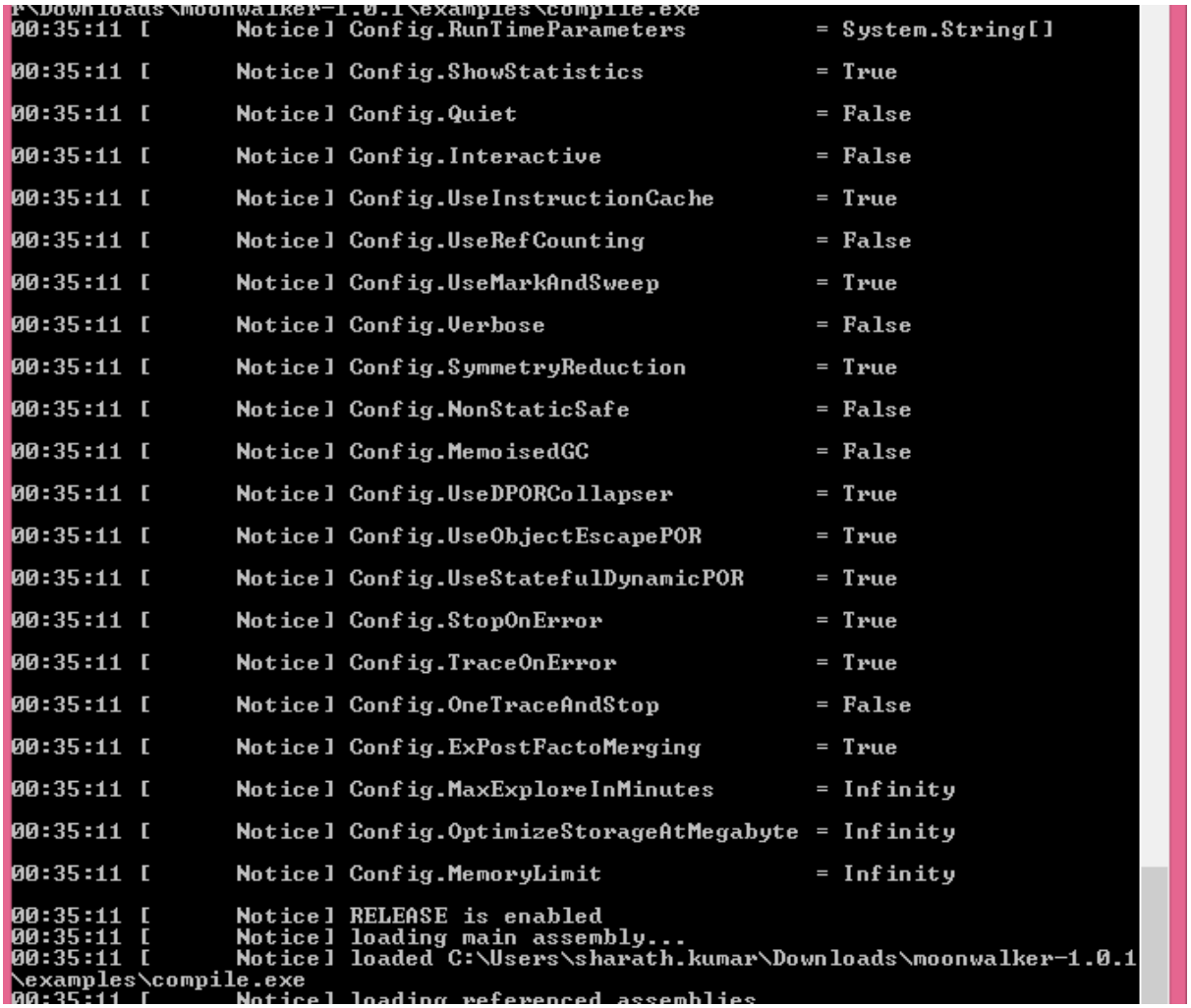


Figure A01: The different panes in the MoonWalker tool

The output with statistics turned on is as shown in Figure A02.

The features displayed in the screen below can be switched on or enabled using the arguments listed in the Help list. The '-h' argument will show the list of arguments that can be used to turn the relevant feature on and achieve the desired output.



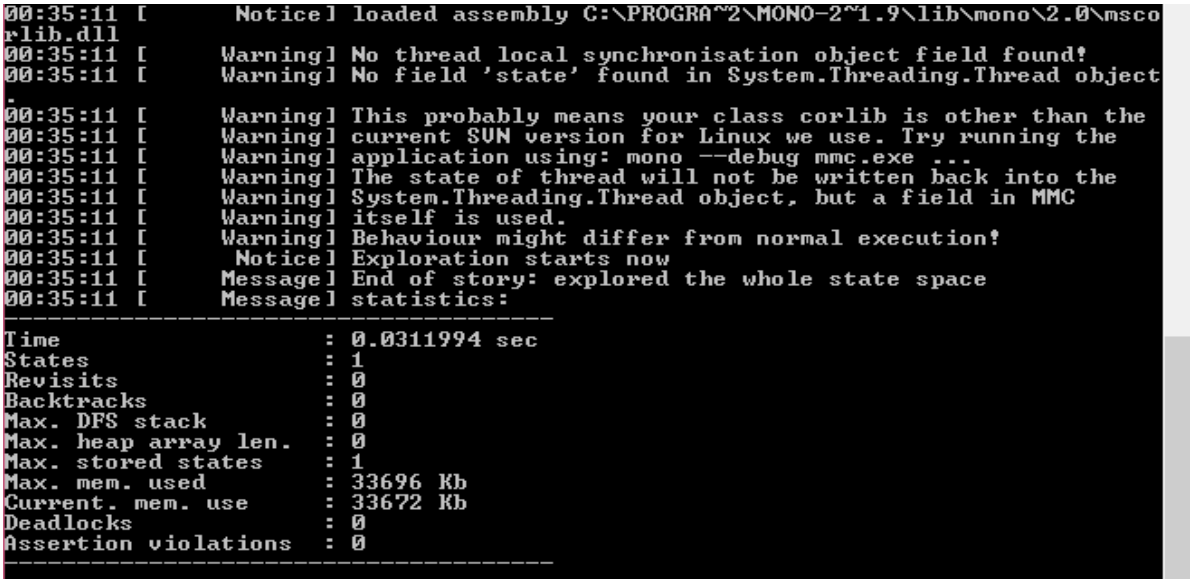


Fig A02: Output screen of MoonWalker with statistics turned on

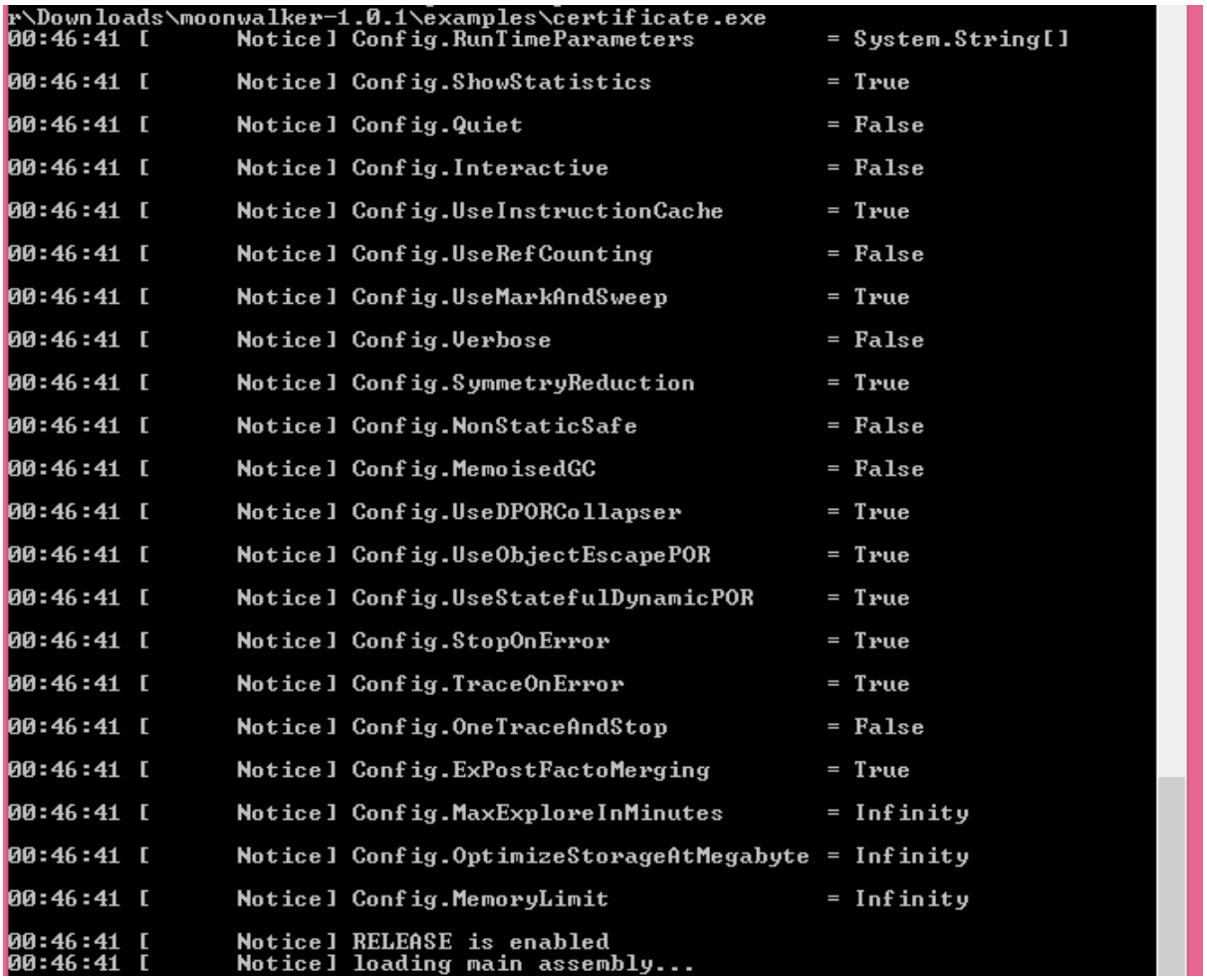
The above figure (Figure A02) shows that there is no major issue with the program currently. Please note that at 35:11 minutes, the “Exploration starts now” refers to the model-checker beginning to check the state-space for any violations. In the following statement it is displayed as “End-of-Story” which refers to the state-space exploration being complete. Once the state-space exploration is complete, the statistical data relating to deadlocks, memory management issues (including heaps, stacks, memory usage) and assertion violations are displayed in detail.

This shows that the compiled code has no problems. From the output, it can be found that the total time taken for the execution of the program (compile.exe) is 0.0312 seconds. Note that the model-checker message says “Exploration starts now”, which means that the model-checker is starting to check for assertion errors and violations after having loaded the necessary DLLs (Dynamic Link Libraries).

The number of stored states is 1. The model-checker enters and stores a state where it has to perform an evaluation. Current-state memory use is about 32.88 MB. This helps us determine how much memory the process uses while performing the model-check and not the memory that the program itself uses.

The displayed statistics suggest that there are no assertion violations or deadlocks. This means that there is no flaw in the logic of the proposed protocol and that the modelling has been successful; thus, the proposed Imposing Fairness Protocol has passed the test.

Given that the compilation of all programs together has been successful and no problems have been spotted, now it is necessary to individually compile every program to check for deadlocks, assertion violations and race conditions. For individual programs as well, the –s argument can be used to list statistics and turn features on or off. The screenshot below (Fig. A03) displays the features that are enabled or disabled.


r\Downloads\moonwalker-1.0.1\examples\certificate.exe
00:46:41 [Notice] Config.RunTimeParameters = System.String[]
00:46:41 [Notice] Config.ShowStatistics = True
00:46:41 [Notice] Config.Quiet = False
00:46:41 [Notice] Config.Interactive = False
00:46:41 [Notice] Config.UseInstructionCache = True
00:46:41 [Notice] Config.UseRefCounting = False
00:46:41 [Notice] Config.UseMarkAndSweep = True
00:46:41 [Notice] Config.Verbose = False
00:46:41 [Notice] Config.SymmetryReduction = True
00:46:41 [Notice] Config.NonStaticSafe = False
00:46:41 [Notice] Config.MemoisedGC = False
00:46:41 [Notice] Config.UseDPORCollapser = True
00:46:41 [Notice] Config.UseObjectEscapePOR = True
00:46:41 [Notice] Config.UseStatefulDynamicPOR = True
00:46:41 [Notice] Config.StopOnError = True
00:46:41 [Notice] Config.TraceOnError = True
00:46:41 [Notice] Config.OneTraceAndStop = False
00:46:41 [Notice] Config.ExPostFactoMerging = True
00:46:41 [Notice] Config.MaxExploreInMinutes = Infinity
00:46:41 [Notice] Config.OptimizeStorageAtMegabyte = Infinity
00:46:41 [Notice] Config.MemoryLimit = Infinity
00:46:41 [Notice] RELEASE is enabled
00:46:41 [Notice] loading main assembly...

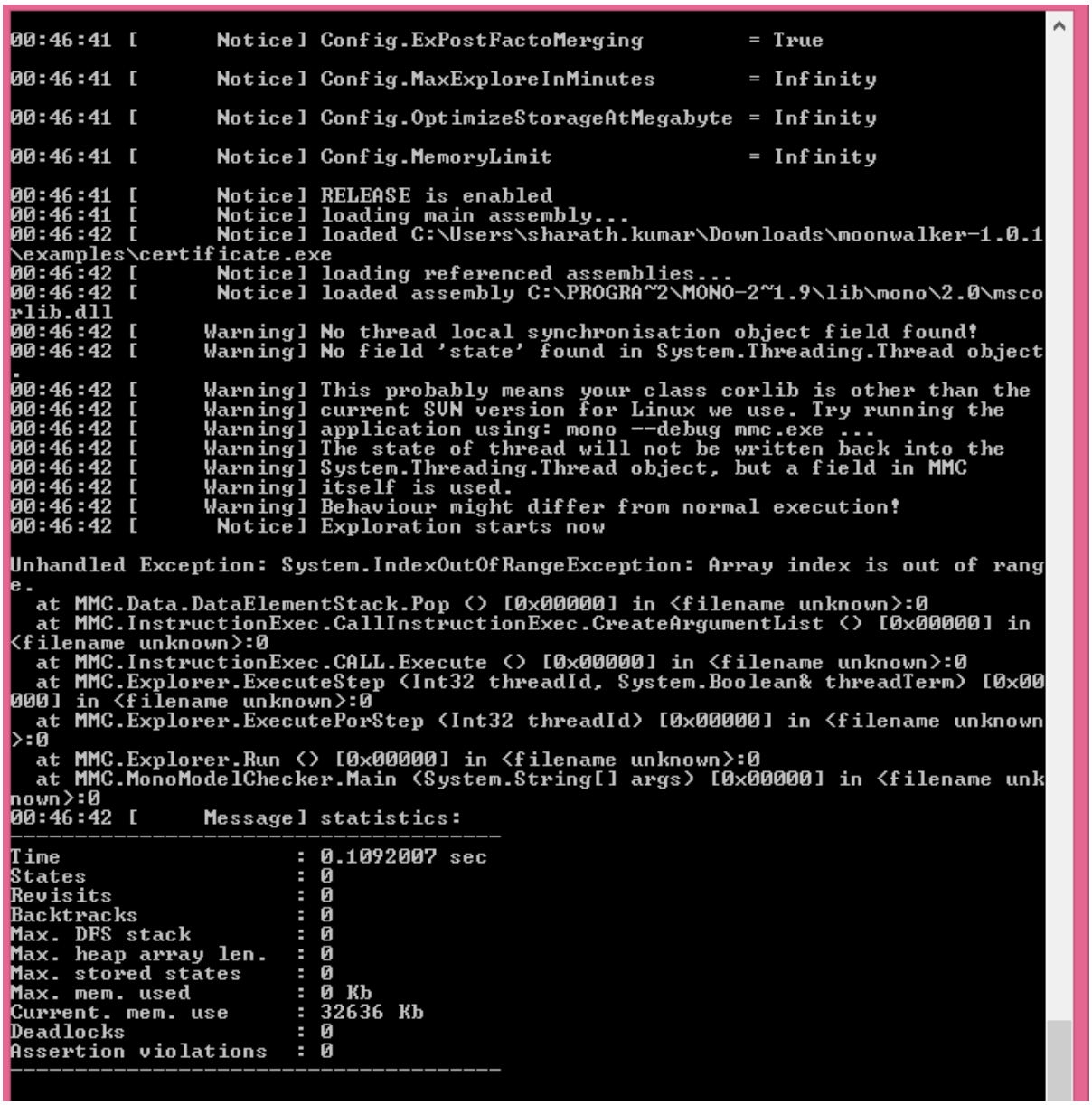
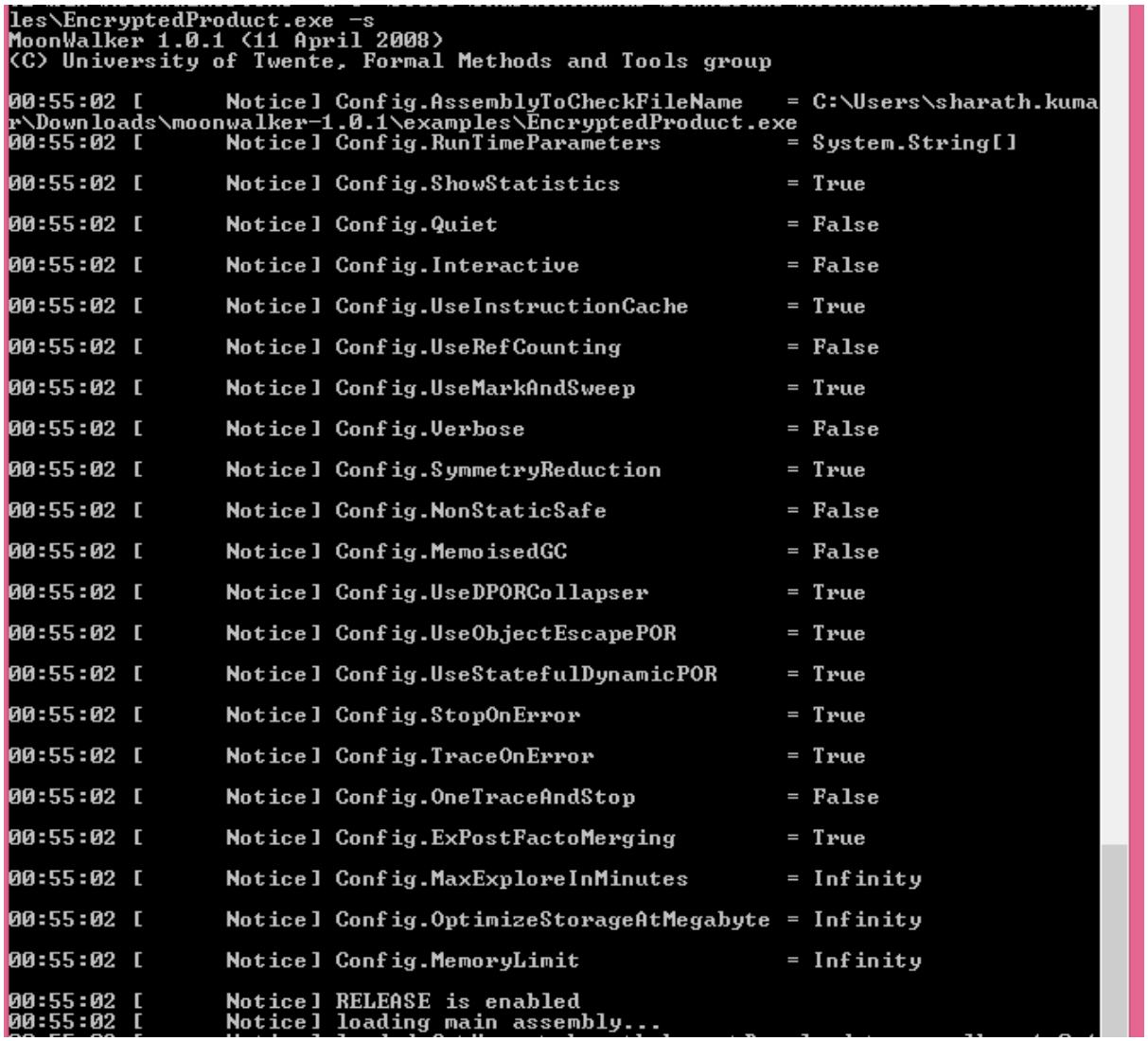


Fig A03: Model-checker output for certificate.exe file

The above screenshot is the model-checker run-through for the certificate.exe file. Like the compile.exe, this module gives us a similar result, showing us that there are no assertion violations or deadlocks.

This module however displays an unhandled exception being encountered while running the compiled program. Unhandled exception is not an assertion violation in modelling, nor is it a

modelling failure; rather, it is an array index – an ‘out of range’ exception. The model itself has been tested and passed without violations or race conditions. Thus, it is only a warning to the user about a probable unwanted behaviour due to the form in which the code is being run through the model – in simple terms, it means that the logic is trying to access an array that does not exist, and once we have defined this array, the exception should not occur. So in other words, the compilation is successful, the modelling is successful, and the exception can be rectified by making sure that during compilation and build, the array sizes are defined and the index is within the bounds of the array.



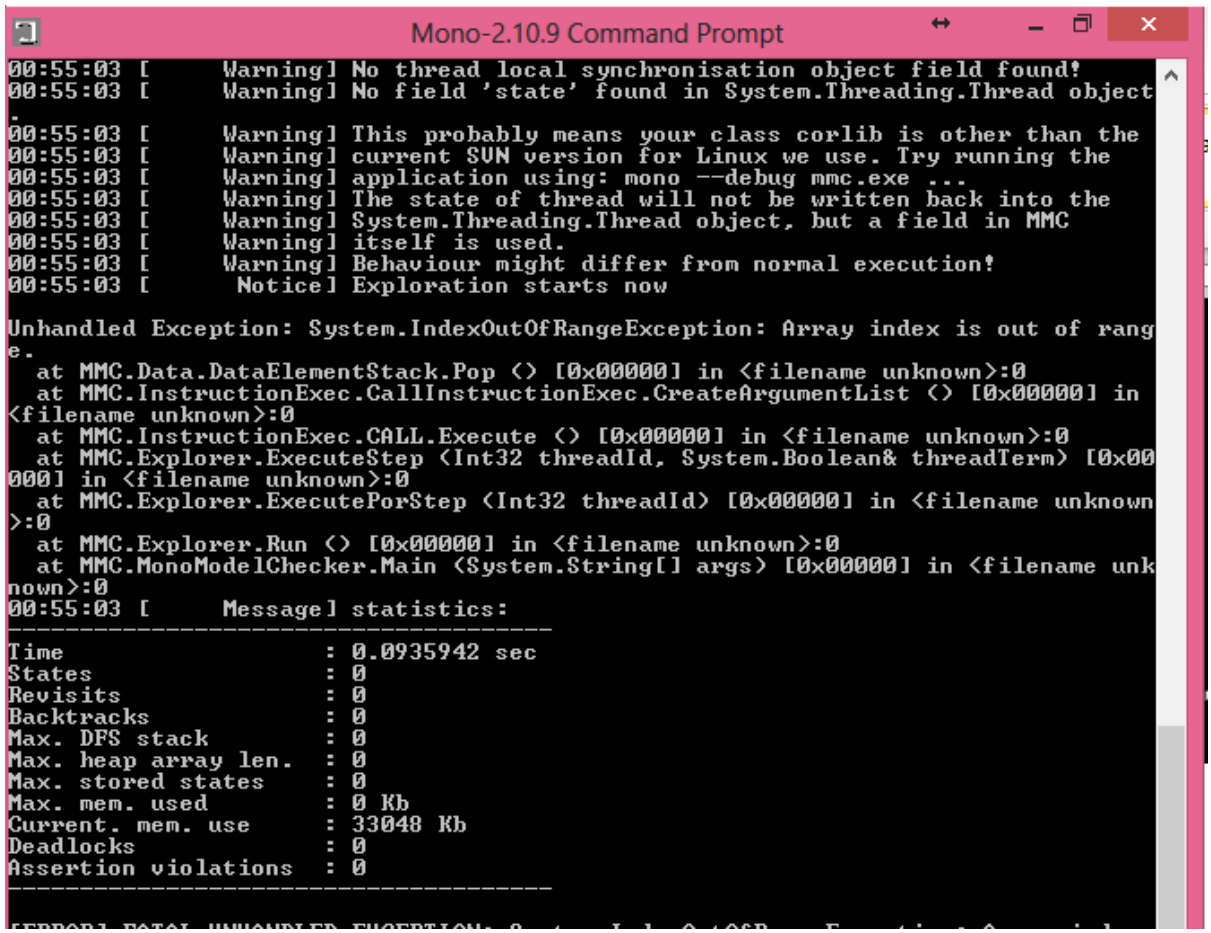
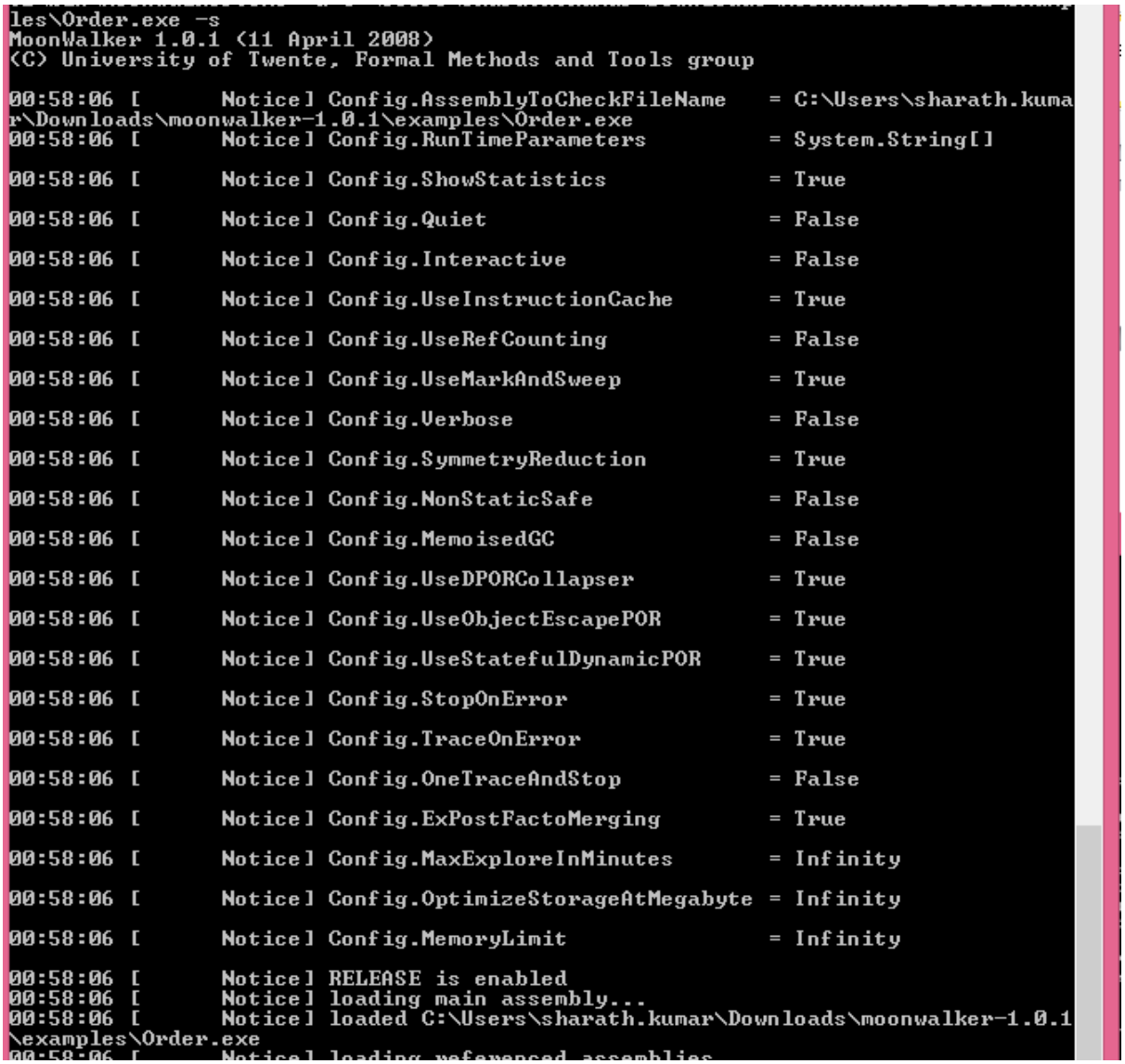


Fig A04: Model checker run for EncryptedProduct.exe file

The above screenshot (Fig. A04) is the model-checker run-through for the EncryptedProduct.exe file. From the above, we can find that this file, as with the other two compilations, has no deadlocks, race conditions or assertion violations.


les\Order.exe -s
MoonWalker 1.0.1 (11 April 2008)
(C) University of Twente, Formal Methods and Tools group
00:58:06 [Notice] Config.AssemblyToCheckFileName = C:\Users\sharath.kuma
r\Downloads\moonwalker-1.0.1\examples\Order.exe
00:58:06 [Notice] Config.RunTimeParameters = System.String[]
00:58:06 [Notice] Config.ShowStatistics = True
00:58:06 [Notice] Config.Quiet = False
00:58:06 [Notice] Config.Interactive = False
00:58:06 [Notice] Config.UseInstructionCache = True
00:58:06 [Notice] Config.UseRefCounting = False
00:58:06 [Notice] Config.UseMarkAndSweep = True
00:58:06 [Notice] Config.Verbose = False
00:58:06 [Notice] Config.SymmetryReduction = True
00:58:06 [Notice] Config.NonStaticSafe = False
00:58:06 [Notice] Config.MemoisedGC = False
00:58:06 [Notice] Config.UseDPORCollapser = True
00:58:06 [Notice] Config.UseObjectEscapePOR = True
00:58:06 [Notice] Config.UseStatefulDynamicPOR = True
00:58:06 [Notice] Config.StopOnError = True
00:58:06 [Notice] Config.TraceOnError = True
00:58:06 [Notice] Config.OneTraceAndStop = False
00:58:06 [Notice] Config.ExPostFactoMerging = True
00:58:06 [Notice] Config.MaxExploreInMinutes = Infinity
00:58:06 [Notice] Config.OptimizeStorageAtMegabyte = Infinity
00:58:06 [Notice] Config.MemoryLimit = Infinity
00:58:06 [Notice] RELEASE is enabled
00:58:06 [Notice] loading main assembly...
00:58:06 [Notice] loaded C:\Users\sharath.kumar\Downloads\moonwalker-1.0.1
\examples\Order.exe

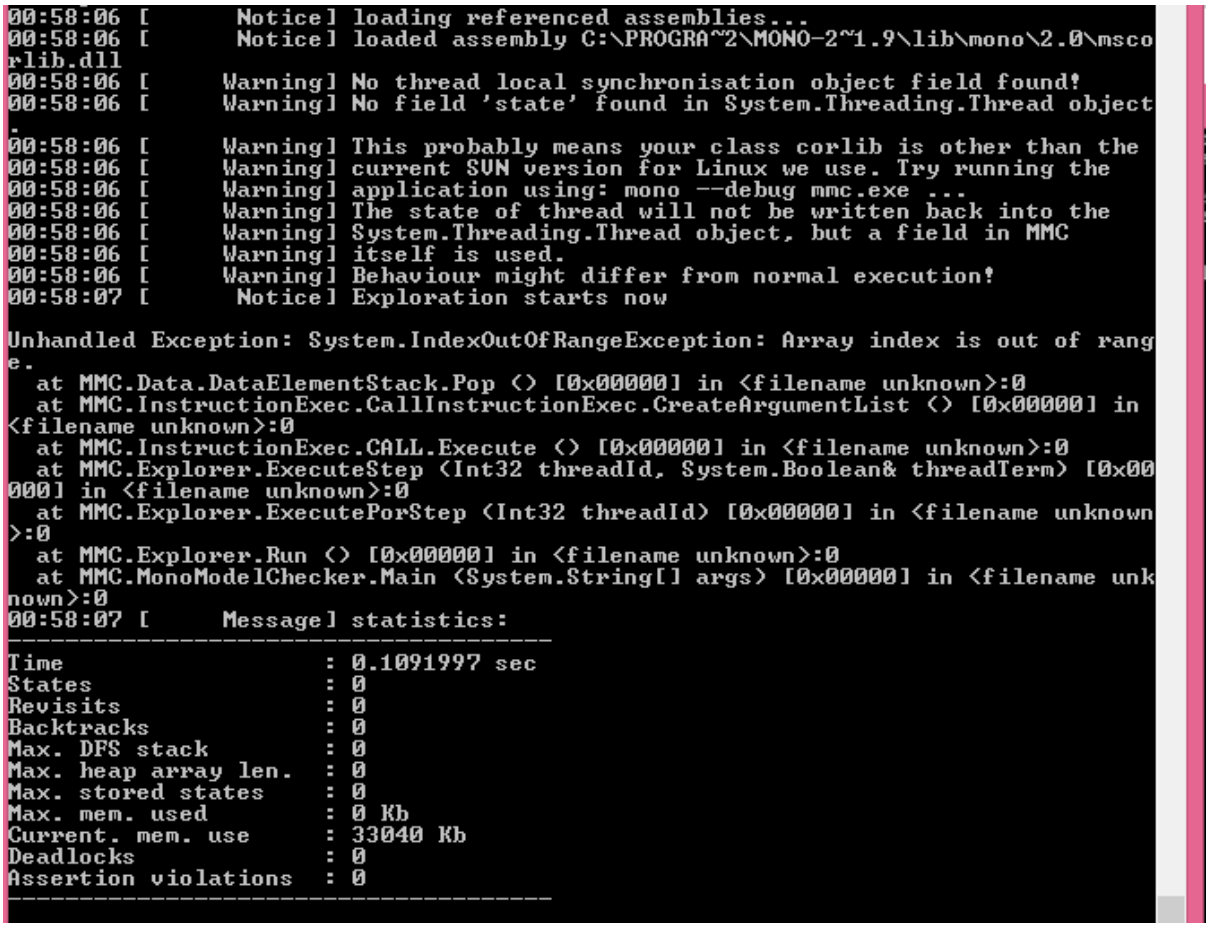
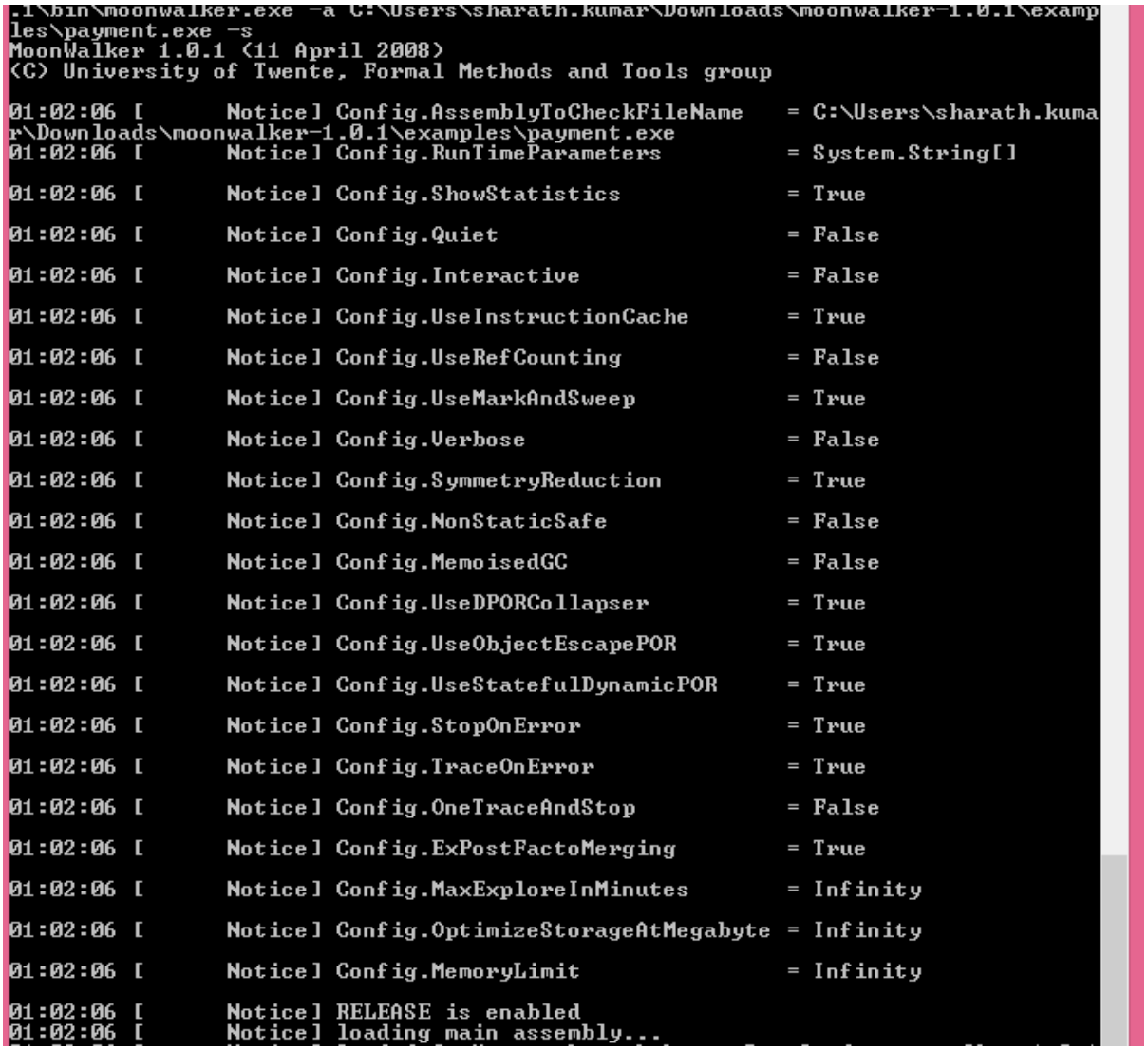


Fig A05: Model checker run for the file Order.exe

The above screenshot (Fig. A05) is the model-checker run-through for the Order.exe file. Again, it can be noted that, as with the other outputs, there are no deadlocks or assertion violations found in this program.


.1\bin\moonwalker.exe -a C:\Users\sharath.kumar\Downloads\moonwalker-1.0.1\examp
les\payment.exe -s
MoonWalker 1.0.1 (11 April 2008)
(C) University of Twente, Formal Methods and Tools group
01:02:06 [Notice] Config.AssemblyToCheckFileName = C:\Users\sharath.kuma
r\Downloads\moonwalker-1.0.1\examples\payment.exe
01:02:06 [Notice] Config.RunTimeParameters = System.String[]
01:02:06 [Notice] Config.ShowStatistics = True
01:02:06 [Notice] Config.Quiet = False
01:02:06 [Notice] Config.Interactive = False
01:02:06 [Notice] Config.UseInstructionCache = True
01:02:06 [Notice] Config.UseRefCounting = False
01:02:06 [Notice] Config.UseMarkAndSweep = True
01:02:06 [Notice] Config.Verbose = False
01:02:06 [Notice] Config.SymmetryReduction = True
01:02:06 [Notice] Config.NonStaticSafe = False
01:02:06 [Notice] Config.MemoisedGC = False
01:02:06 [Notice] Config.UseDPORCollapser = True
01:02:06 [Notice] Config.UseObjectEscapePOR = True
01:02:06 [Notice] Config.UseStatefulDynamicPOR = True
01:02:06 [Notice] Config.StopOnError = True
01:02:06 [Notice] Config.TraceOnError = True
01:02:06 [Notice] Config.OneTraceAndStop = False
01:02:06 [Notice] Config.ExPostFactoMerging = True
01:02:06 [Notice] Config.MaxExploreInMinutes = Infinity
01:02:06 [Notice] Config.OptimizeStorageAtMegabyte = Infinity
01:02:06 [Notice] Config.MemoryLimit = Infinity
01:02:06 [Notice] RELEASE is enabled
01:02:06 [Notice] loading main assembly...

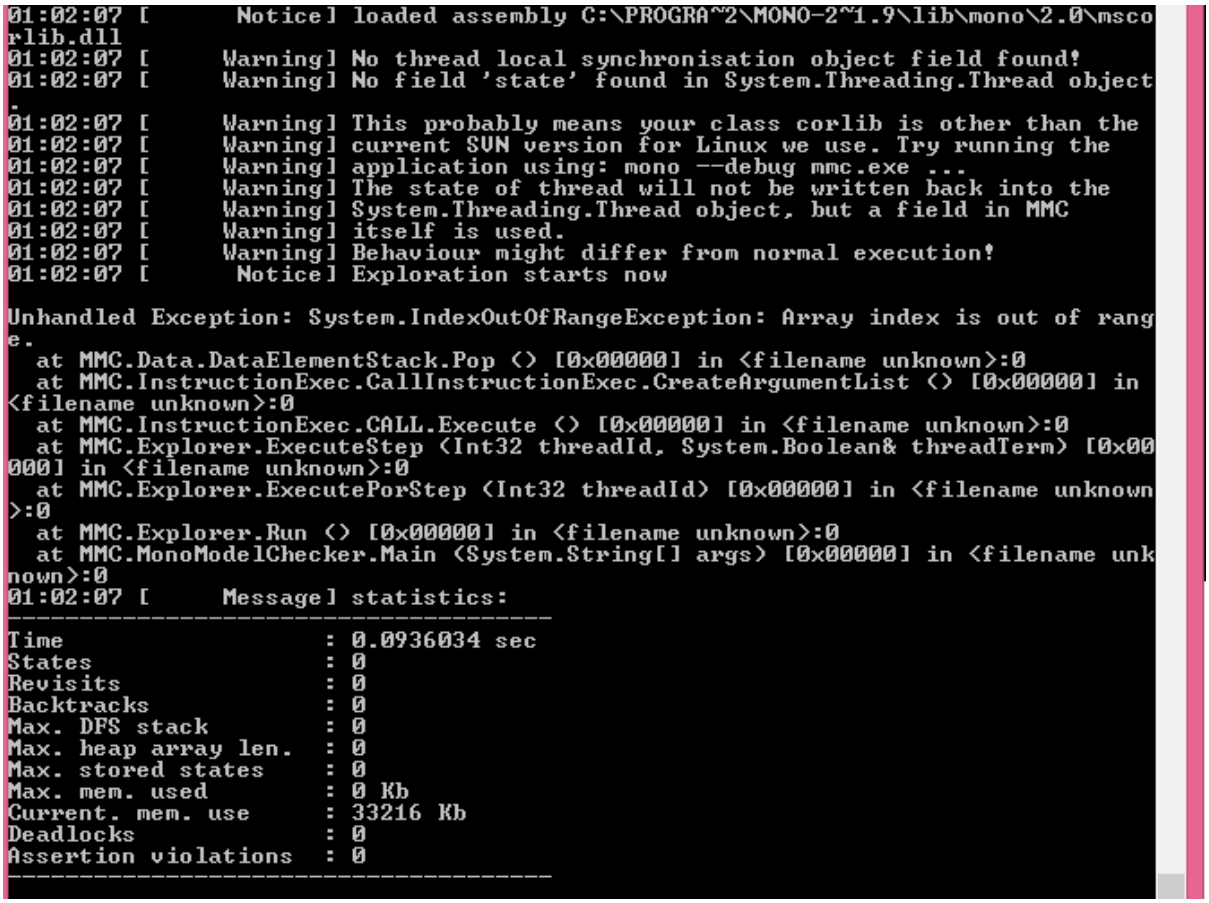
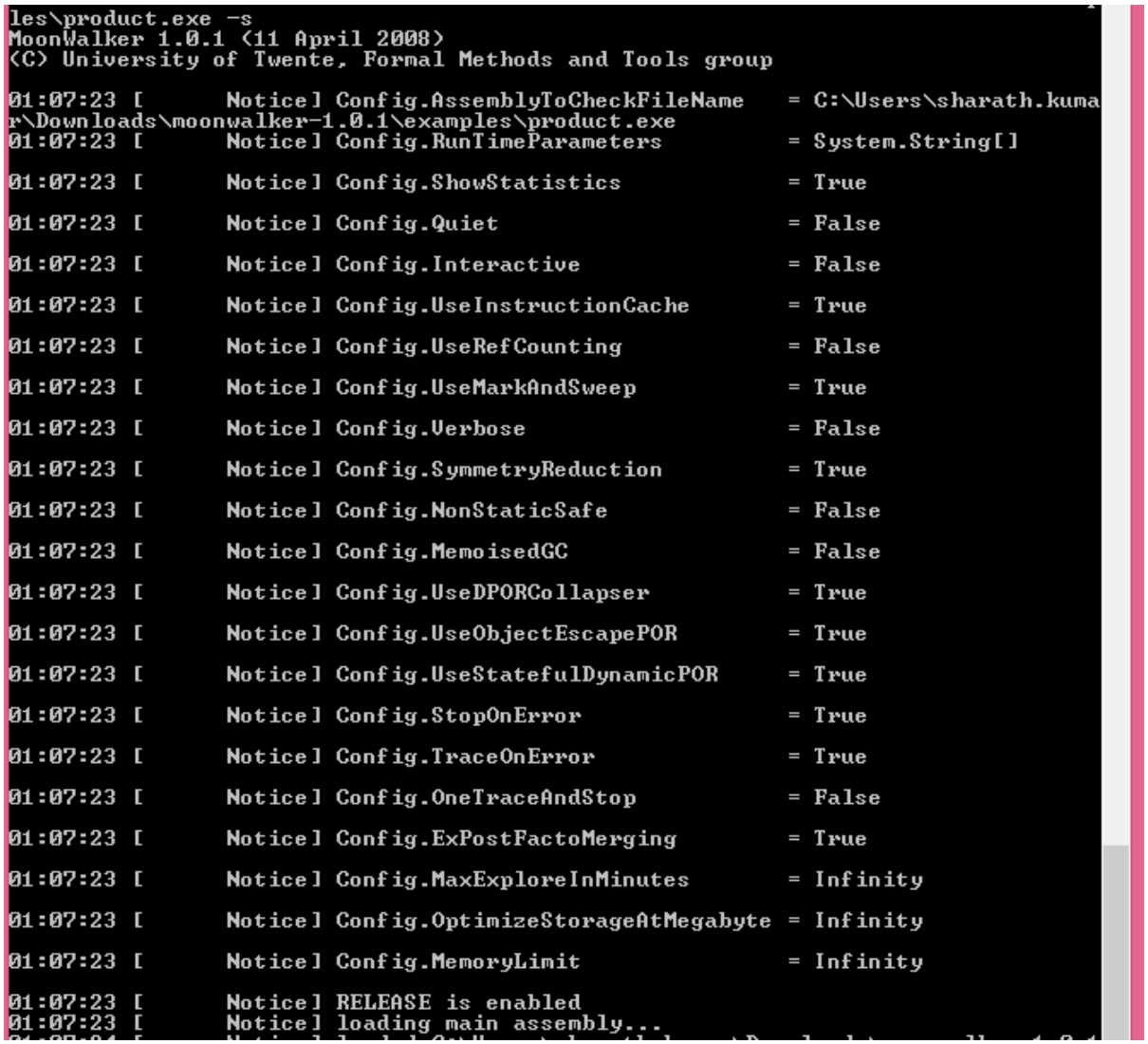


Fig A06: Model checker run for Payment.exe file

The above screenshot (Fig. A06) is the model-checker run-through for the Payment.exe file. This gives us a similar result, as there are no assertion violations or deadlocks.


les\product.exe -s
MoonWalker 1.0.1 (11 April 2008)
(C) University of Twente, Formal Methods and Tools group
01:07:23 [Notice] Config.AssemblyToCheckFileName = C:\Users\sharath.kuma
r\Downloads\moonwalker-1.0.1\examples\product.exe
01:07:23 [Notice] Config.RunTimeParameters = System.String[]
01:07:23 [Notice] Config.ShowStatistics = True
01:07:23 [Notice] Config.Quiet = False
01:07:23 [Notice] Config.Interactive = False
01:07:23 [Notice] Config.UseInstructionCache = True
01:07:23 [Notice] Config.UseRefCounting = False
01:07:23 [Notice] Config.UseMarkAndSweep = True
01:07:23 [Notice] Config.Verbose = False
01:07:23 [Notice] Config.SymmetryReduction = True
01:07:23 [Notice] Config.NonStaticSafe = False
01:07:23 [Notice] Config.MemoisedGC = False
01:07:23 [Notice] Config.UseDPORCollapser = True
01:07:23 [Notice] Config.UseObjectEscapePOR = True
01:07:23 [Notice] Config.UseStatefulDynamicPOR = True
01:07:23 [Notice] Config.StopOnError = True
01:07:23 [Notice] Config.TraceOnError = True
01:07:23 [Notice] Config.OneTraceAndStop = False
01:07:23 [Notice] Config.ExPostFactoMerging = True
01:07:23 [Notice] Config.MaxExploreInMinutes = Infinity
01:07:23 [Notice] Config.OptimizeStorageAtMegabyte = Infinity
01:07:23 [Notice] Config.MemoryLimit = Infinity
01:07:23 [Notice] RELEASE is enabled
01:07:23 [Notice] loading main assembly...

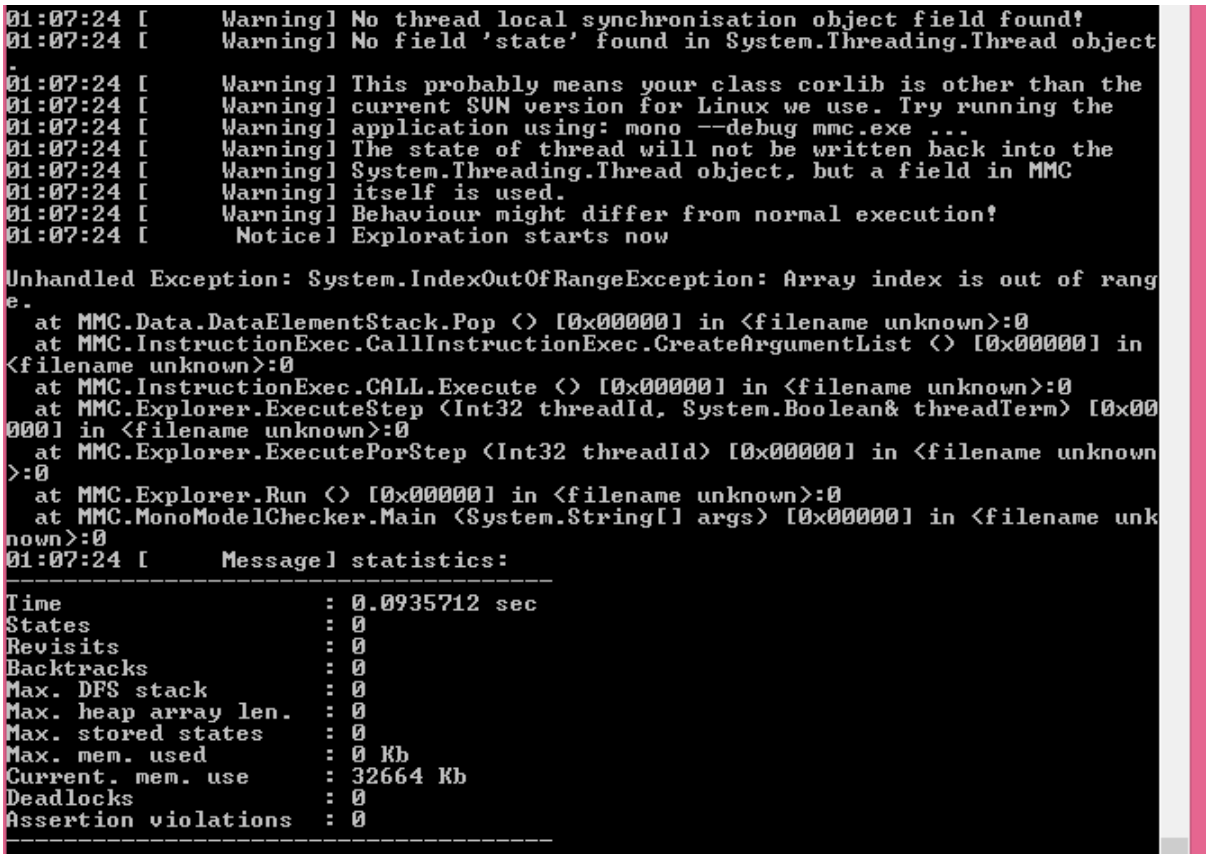
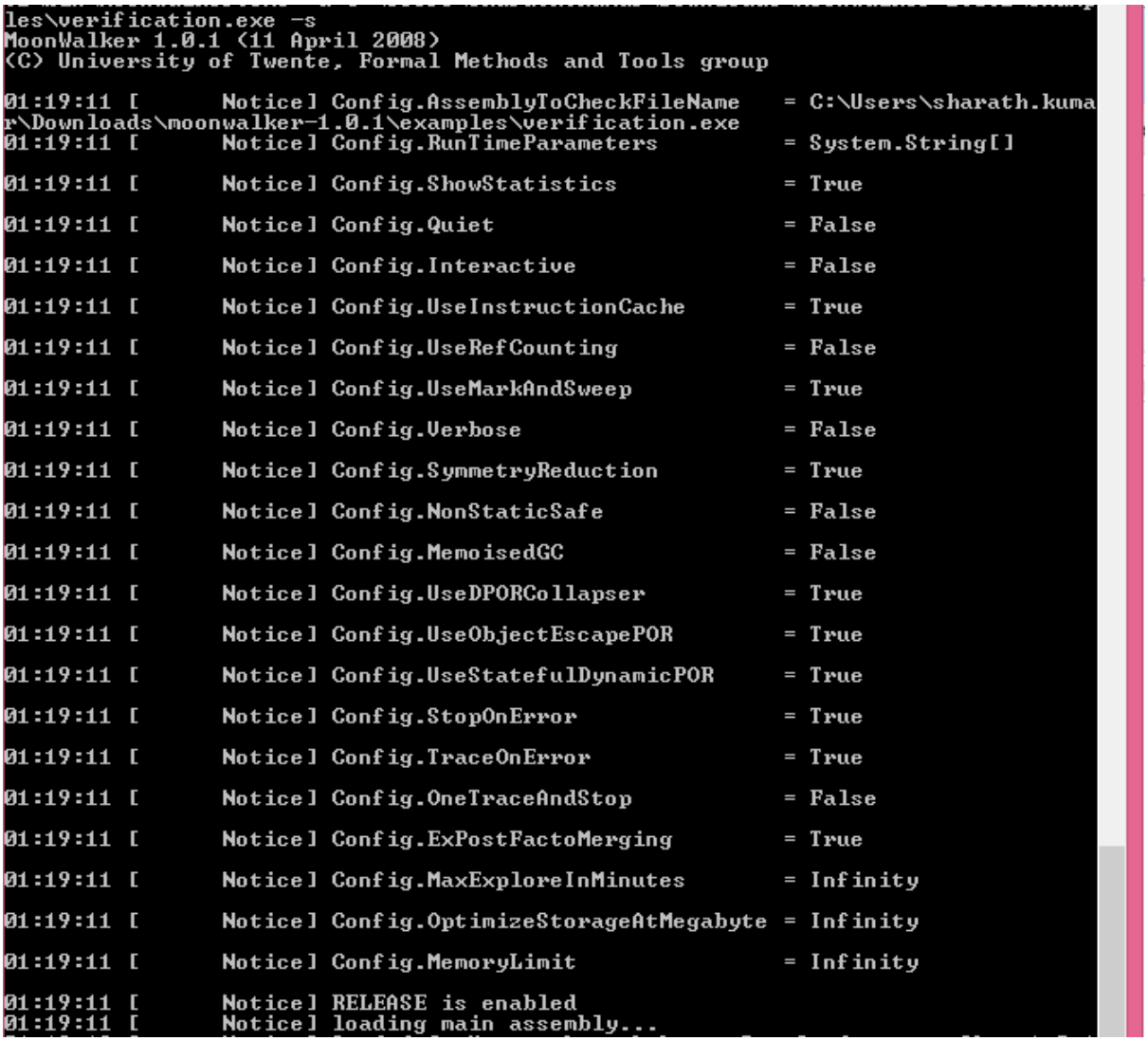


Fig A07: Model checker run for Product.exe file

The above screenshot (Fig. A07) is the model-checker run-through for the Product.exe file. This gives us a similar result, as there are no assertion violations or deadlocks.


les\verification.exe -s
MoonWalker 1.0.1 (11 April 2008)
(C) University of Twente, Formal Methods and Tools group
01:19:11 [Notice] Config.AssemblyToCheckFileName = C:\Users\sharath.kuma
r\Downloads\moonwalker-1.0.1\examples\verification.exe
01:19:11 [Notice] Config.RunTimeParameters = System.String[]
01:19:11 [Notice] Config.ShowStatistics = True
01:19:11 [Notice] Config.Quiet = False
01:19:11 [Notice] Config.Interactive = False
01:19:11 [Notice] Config.UseInstructionCache = True
01:19:11 [Notice] Config.UseRefCounting = False
01:19:11 [Notice] Config.UseMarkAndSweep = True
01:19:11 [Notice] Config.Verbose = False
01:19:11 [Notice] Config.SymmetryReduction = True
01:19:11 [Notice] Config.NonStaticSafe = False
01:19:11 [Notice] Config.MemoisedGC = False
01:19:11 [Notice] Config.UseDPORCollapser = True
01:19:11 [Notice] Config.UseObjectEscapePOR = True
01:19:11 [Notice] Config.UseStatefulDynamicPOR = True
01:19:11 [Notice] Config.StopOnError = True
01:19:11 [Notice] Config.TraceOnError = True
01:19:11 [Notice] Config.OneTraceAndStop = False
01:19:11 [Notice] Config.ExPostFactoMerging = True
01:19:11 [Notice] Config.MaxExploreInMinutes = Infinity
01:19:11 [Notice] Config.OptimizeStorageAtMegabyte = Infinity
01:19:11 [Notice] Config.MemoryLimit = Infinity
01:19:11 [Notice] RELEASE is enabled
01:19:11 [Notice] loading main assembly...

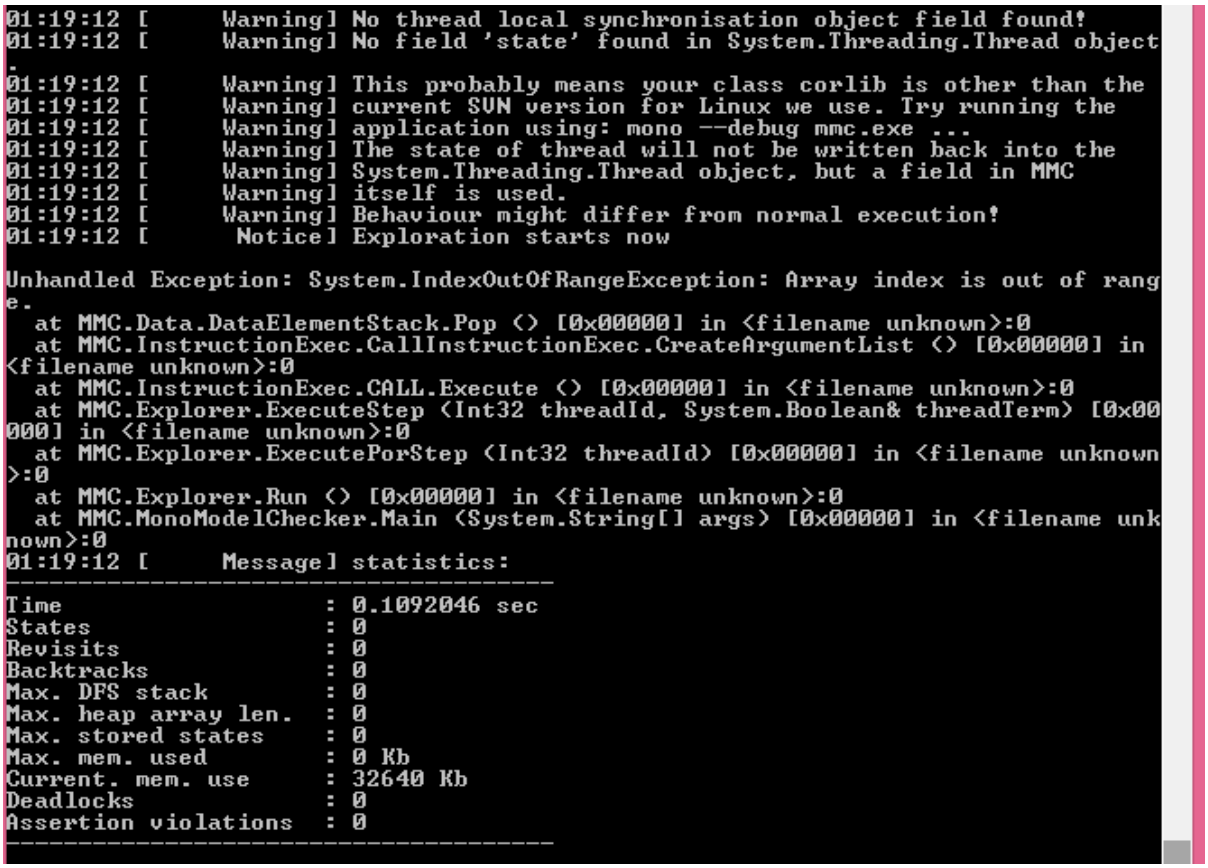


Fig A08: Model-checker run for Verification.exe file

The above (Fig. A08) screenshot is the model-checker run-through for the Verification.exe file. This gives us a similar result, as there are no assertion violations or deadlocks.