A Review and Future Research Directions of Secure and Trustworthy Mobile Agent-based E-marketplace Systems

Ahmed Patel[*, 1, 2], Wei Qi[1] and Christopher Wills[2]

[1]*Department of Computer Science*
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
(The National University of Malaysia)
43600 Bangi, Selangor Darul Ehsan
Malaysia

[2]*Faculty of Computing Information Systems and Mathematics*
Kingston University
Penrhyn Road
Kingston upon Thames KT1 2EE
United Kingdom

apatel@ftsm.ukm.my, *qiwei820@gmail.com*, *ccwills@kingston.ac.uk*

Abstract

Purpose – Agent technology has generated a lot of interest in recent years, including mobile agent technology with its advantage of being able to support mobility, which can reduce network latency and dependency on network availability. Therefore, a number of mobile agent-based e-commerce applications have been constructed. Mobile agent-based e-marketplaces are e-commerce trading platforms which represent the business models and processes for buyers and sellers to trade goods and provide services via the extended distributed channels of the Web over the Internet and mobile networks. However, mobile agents introduced a series of security and privacy issues such as the protection of the computing and network platforms and the host that runs the mobile agent against attacks which can harm or use its resources without permission as well as the essential protection necessary to guard mobile agents against malicious hosts that might alter the information it carries when it visits other hosts in its itineraries, and possibly siphon or transfer the client's privacy information. This raises the need to provide secure and safe information security systems through the use of firewalls, intrusion detection and prevention systems, encryption, authentication and other hardware and software solutions. To solve these problems, we propose a framework which includes safe, secure, trusted and auditable services, as well as forensic mechanisms to provide audit trails for digital evidence of transactions and protection against malicious and illegal activities.
Design/methodology/approach – This paper reviews the literature as the foundation and knowledge base for the proposed framework and system of secure and trustworthy mobile agent-based e-marketplaces. It consists of the current state of the art taxonomy for the classified mobile agent-based frameworks for e-marketplace trading, underlying supporting systems, e-payment systems and the essential issues related to auditable and digital forensic services.
Findings – The current knowledge shows that there is a serious lack of auditable and digital forensic services to make secure and trustworthy mobile agent-based e-marketplaces systems. We draw conclusions and

[*]Corresponding author & [2]Visiting Professor at Kingston University in the UK

highlight further research work which is ongoing and new work that needs to be performed.
Originality/value – This paper perceives the needs to define the requirements for secure and trustworthy mobile agent-based e-marketplaces and proposes a framework to design effective systems using the latest techniques and technologies.
Keywords – Audit, digital forensics, e-marketplace, mobile agents, privacy, security, trust

1. Introduction

With the rapid development of the Internet and Web technologies, more and more new business applications and strategies are being developed to facilitate and increase the use of electronic global business and e-market trading. The e-marketplace is a flexible and efficient approach to help companies or corporations to extend their businesses to reach larger markets without regional boundaries. A typical e-marketplace consisting of a Web portal which uses only aggregate e-shops and supports limited services such as e-payment system and brokering service does not suffice for today's challenging business communities. E-marketplace participants expect more services to be available all the time, not only from fixed desktop computers, but also preferably from their mobile devices.

Mobile Agent (MA) is a software application that can work autonomously and has the capability to move from one device to another to execute and perform tasks on different hosts for their owners in a computer network. It consumes bandwidth only when it moves but can continue to execute tasks after the move, even if it loses network connectivity with its principals (Mahmoud 2006). Using a mobile agent can help reduce the network usage, reduce the dependency on network availability and avoid the network latency (Alfalayleh and Brankovic 2004). Consequently, a mobile agent-based e-marketplace can be regarded as a good business "model" and platform for buyers and sellers to perform transactions of goods and services via the extended distributed channels over the Internet or mobile network. Mobile agent technology has its own limitations. Even though mobility can partially avoid network latency and possibly increase the fairness in application with bounded response times to offer e-marketplace trading by/to buyers and sellers either on the move or in hostile non-permanent environments, mobile agents moving around the network are known to be a threat to a remote host. They raise a number of security issues such as malicious agents and servers, information integrity, etc. Security is one essential factor to be concerned with when we develop a framework for mobile agent-based e-marketplace system. Also to be addressed within the context of security is the privacy, safety and trust issues in personal confidential information protection, payment processing, managing and regulating legitimate trading and the transparent user interface.

In a business-to-business (B2B) market, there are several e-market models, namely, a buy-site model for a buyer, a seller-site model is seller-biased, and a third-party model which does not take sides and usually is managed and maintained by a company or consortium. Particularly in a third party e-marketplace, each participant, that is, buyer and seller can be associated with specific goal-driven MAs to facilitate deals. The infrastructure services can be implemented as management agents which act as registration authority, certificate authority, directory service, brokering agent, payment gateway, and delivery services (Jailani et al. 2008). Figure 1 shows an example of a third party e-marketplace architecture using mobile agent which offers infrastructure services which amongst others include certificate authority, secure electronic payment, trustworthy and digital forensic agent for tracing transactions. It is a very complex environment which needs a very strong, secure, trusted base.

Therefore, the goal of this paper is to review the literature as the foundation and knowledge base for the proposed framework and system of secure and trustworthy mobile agent-based e-marketplaces. It consists of the current state of the art taxonomy for the classified mobile agent-based frameworks for e-marketplace trading, underlying supporting systems, e-payment systems and the essential services and issues such as the security, privacy, safety and trust issues related to auditable and digital forensic services.

The paper is organized as follows: Section 2 describes the problem statement through a scenario pertaining to this research project. Section 3 describes the current status of mobile agent-based e-marketplace that includes the list of security requirements for mobile agent-based e-marketplaces, followed by the infrastructure services and the e-payment systems for mobile agent-based e-marketplace. Section 4 presents the review and the issues of the security, privacy, trustworthy and safety aspects for making safe e-trading possible in an e-marketplace. Section 5 gives a detailed description of the auditable and forensic services for e-marketplace. Section 6 presents a discussion of further research for more sophisticated requirements and design for auditable and forensic services for e-marketplace. Finally, an overall conclusion is given in

Section 7.

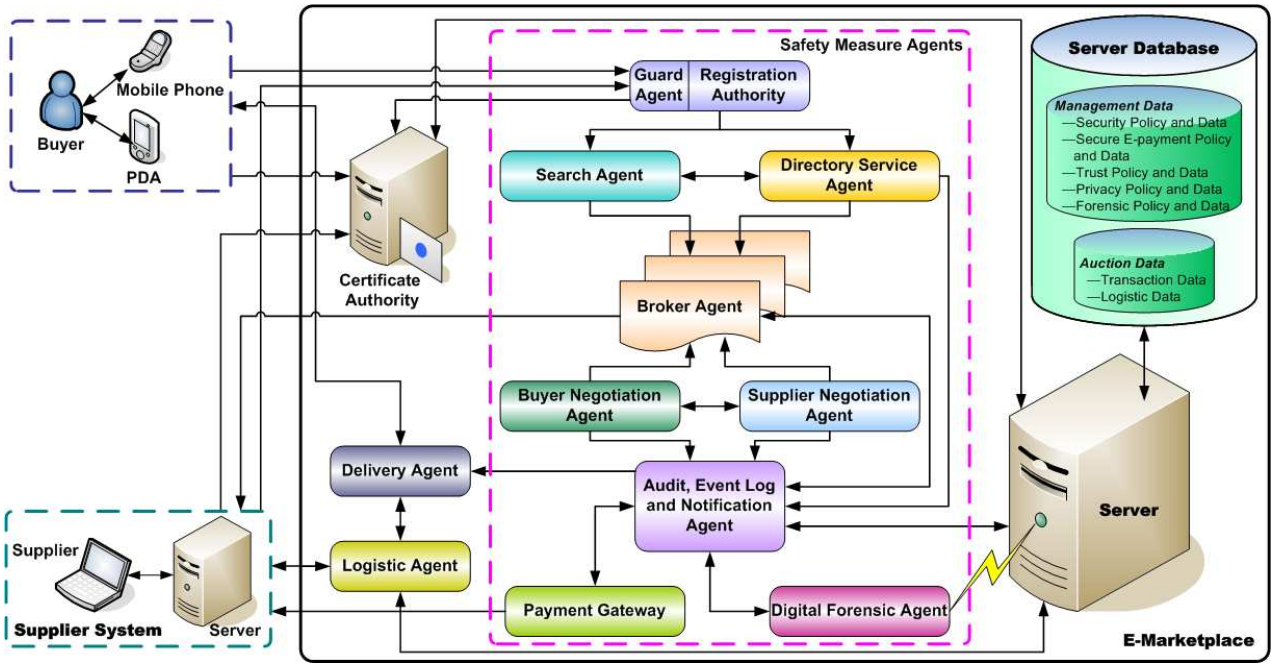

Figure 1. Safety Measure E-marketplace Framework Scenario

2. Problem Statement & Scenario

The development of the architecture for an e-marketplace requires a new design paradigm, improved integration architectures, and services (Ghenniwa and Huhns 2005). In this architecture, the e-marketplace is a cooperative distributed system composed of economically motivated software agents that interact cooperatively or competitively, find and process information, and disseminate it to humans and to other agents. In addition, it must provide support for common economic services and transactions, such as dynamic pricing, negotiation, automated supply chains, as well as other e-marketplace service infrastructure to ensure secure, trusted and reliable transactions.

Although several research works have been dedicated to the design of agent-based marketplaces, the lack of standards for an agent-based e-marketplace framework reflects that there are still many issues that need to be resolved before a standard could be defined for such a framework. This also includes the associated protocols for mobile agents to perform e-marketplace activities, keeping in view that the e-marketplace is a hostile trading environment that must be made safe, secure, trusted and auditable. It must also meet the requirements of mobile users whose expectation of e-marketplace services to be available in mobile computing devices and mobile networks that incur high communication cost and/or low bandwidth within bounded target security conditions to establish fully-fledged goal-driven agent based e-marketplace. Among the major problems to be solved, is that of defining the framework together with all of the safe, secure, trusted and auditable services, including forensic mechanisms for responding to and proofing against illegal activities.

3. Review on Mobile Agent-based E-marketplace Frameworks and Systems

Mobile agent has been proposed in many distributed applications as a useful technology. It is very applicable in e-marketplace trading. MAs are defined as objects that have behaviour, state and location (Kannammal and Iyengar 2007) but without seriously taking security into account. As Jailani et al. (2008) mentioned there are many different mobile agent-based frameworks but none have brought all the important security related issues of privacy, security, auditability etc., together into a single consistent framework. This is addressed below.

3.1. Current Status of Mobile Agent-based E-marketplace

The failure of accommodating the end-user or system processes to use mobile e-trading and its security, audit and forensic features in a seamless and transparent way is one major weakness in today's mobile agent-based e-marketplace systems usage as Jailani et al. (2008) have reported. For instance, Chen et al. (2000) proposed a mobile agent-based e-commerce process. They have analysed the advantages and reasons for applying the mobile agent in e-commerce systems. Their research work presented the working flow for mobile agent-based e-commerce, listed each agent for the system and showed how they work. They indicated the system should figure out the relations between security, autonomy and open system issues with the combination of secure protocol in e-commerce as their future research. While Zhao et al. (2007) proposed a mobile agent-based e-commerce model (MA-ECM) which focused on the security, integrity and confidentiality of mobile agent to secure the trading transactions. They embedded the cryptography technique into their framework such as message digest (MD5), RSA (Rivest, Shamir and Adleman 1978) and Rijindeal algorithm to make the system more secure. The system implementation was executed by using Aglets (IBM 2004) mobile agent platform and Java programming language.

High risk security threats appear with strong mobility. To reduce the security threats of a mobile agent, Zhang and Lin (2005) proposed a framework for e-commerce that uses both single hop and multi-hop to reduce the risks. The first phase uses multi-hop for information collection where mobile agent does not take any sensitive information. The second phase uses single hop to take the sensitive information to reduce the security risks. In another way, Wang et al. (2004) proposed a solution to secure the mobile agent-based e-commerce. They present the secure authentication infrastructure by using Public Key Infrastructure (PKI) and introduced an integrity protection and confidentiality service. This protection solution is based on Multiple Hop_Adaption (MH_A) integrity protection with regards to PKI limit.

It is important to ensure that the information carried by a mobile agent or stored on a platform is accessible only to authorized parties (Kannammal and Iyengar 2007). To address such privacy and trust issues from both user and system perspectives, Yu and Li (2006) proposed an encrypted transmission mechanism for mobile agent-based system which overcomes the weakness of traditional communications for the distribution of data encryption key without going through a third-party. While Zhou (2007) proposed a history event-based security authentication method therefore to resolve some security services problem in mobile agent-based cooperative e-commerce. They used authentication model – SPL (Security Policy Language) as their security strategy and this strategy would be applied in their certification system.

To protect or guard against the malicious attack, the frameworks and systems should embed the security protocols. Song and Korba (2003) proposed the security communication architecture for mobile agents in e-commerce application. They analyzed the risk of active and passive attacks for mobile agents and e-commerce and proposed a security protocol to provide a secure communication for the MAs when they move to different security environments in order to deal with some e-commerce processing like ordering payment, delivery of purchase confirmation, etc.

The frameworks and systems described above include some aspects of security, trust, autonomy, privacy and forensic issues, but do not go into any great detail and exposition, while Patel (2010) proposed a much more detailed secure and auditable agent-based framework for mobile users. They investigate the requirements and analyze the architecture needed to define a secure and auditable agent-based framework via auditable and forensic investigations. They exemplified the framework and protocols with an auction e-marketplace as the e-commerce application and presented scenarios to make their point. They defined the essential requirements for the secure and auditable agent-based e-marketplace as well as requirements for mobile e-commerce environment. Table 1 shows the summaries of the security requirements for agent marketplace.

Table 1 Security requirements for e-marketplaces

Features	Functions
Security	Authentication, authorization, confidentiality, integrity, system defense
Privacy	Anonymity, identity management, 'linkability', Privacy Enhancing Technologies (PETs), reputation, pseudonyms and 'unobservability'
Safety	System safety (backup system) and payment safety (limits of transaction)

Trust	Certificate authority, payment managers, secure electronic payment, authentication
Auditing	Complete auditing system for buyer-seller and the transaction services
Digital forensics	Accountability, traceability, post-active, pre-active investigation system
Malicious agent	Communication, migration, information, malicious agent and server

3.2. Infrastructure Service of Mobile Agent-based E-marketplace

E-marketplaces offer a wide variety of ancillary services required by the members of the trading community, such as authenticating buyers and sellers, streamlining procurement workflow, managing risk, and providing settlement, conflict resolution, and logistical services (Jailani et al. 2008). Three major services for e-marketplace are categorized by Bakos (1998), matching buyers and sellers, facilitating transactions and providing institutional infrastructure. The intermediaries usually provide the first two services, while the last is usually provided by a regulation authority.

Matching buyers and suppliers in e-marketplace provides some very significant services to buyers and sellers which involve how to determine products offerings by specifying features or aggregation of different products; searching for price and product information and discovering and negotiating price.

Facilitating transaction is associated with market transactions such as delivery of information, goods or services to buyers, settlement and trust services.

Institutional infrastructure specifies the rules, regulations and laws that govern market transactions. This involves the issues related to contract law, commercial code and intellectual property protection.

From what have been set out above, the proposed e-marketplace will fulfill the first and second infrastructure services. Based on these infrastructure services, the e-marketplace can be expanded into different types through different technologies. Table 2 shows the summaries of different types of e-marketplace (Jailani et al. 2008).

Table 2 Summaries of e-marketplace

Types of E-marketplace	Features
Buy-side e-marketplace	Use the e-marketplace facilities to procure products or services needed by their organizations via immediate buying methods and procurement.
Sell-side e-marketplace	Sell products and services from an organization to other organizations via a transaction mechanism that is usually found in an e-business application.
Third party e-marketplace	Different types of companies or organizations manage an e-marketplace computer server and the service infrastructures required by an e-marketplace.
Vertical and Horizontal Marketplace	Adds value by managing the interactions between buyers and sellers in a particular industry sector.

These infrastructure services are implemented by using Aglets platform. This platform is widely used as a test-bed for implementing agent-based systems. For example, we apply the IBM Aglets as our mobile agent platform for the system implementation. Table 3 shows the features that are needed for our electronic marketplace were satisfied by the Aglet model (Dasgupta et al. 1998):

1 *Mobility.* Aglet provides a simple Java API for mobility.

2 *Autonomy.* Aglet can make intelligent decisions and run on any machine.

3 *Response time.* Aglet has rapid response time.

4 *Concurrency.* Aglet can dispatch worker agent simultaneously.

5 *Local Interaction.* Aglet can interact with local entities and also the remote entities.

3.3. E-payment Systems for E-marketplace

Electronic Payment System is a very important component of electronic marketplace. It applies to all e-marketplace business models such as B2C, B2B, B2G, C2G and C2C. For example, B2C model supports online payment for goods and services, where B2B serves as an integral part of financial supply chain. E-payments are the paperless method of making payment processes faster and cheaper than the traditional paper-based payment instructions. Therefore, e-payments serve as the key for Internet shopping. Without electronic payment systems, e-marketplace is not complete or at least not practical as a revenue source of a company.

In e-payment systems, there are four major actors in the electronic payment process, the payer, payee, banks and trusted third party. A payer is a person who makes a payment to payee. A payee is a person who receives payment through any form of money transfer methods. A Trusted Third Party (TTP) is often employed to facilitate trust in commercial transactions. A bank is a financial institution that is licensed to deal with money. The bank also can be a TTP. Without any of these four actors, the e-payment process cannot proceed.

The complexity of e-commerce transactions has been growing rapidly in the last few years. Therefore, different payment systems have appeared one after another. The electronic payment system can be broadly divided into four general types:

1. *Online Credit Card Payment System.* This type of payment system has been widely accepted by consumers and merchants throughout the world, and by far the most popular methods of payments especially in the retail markets (Laudon and Traver 2002).
2. *Electronic Cheque System.* Digital chequeing payment system seeks to extend the functionality of existing chequeing accounts for use as online shopping payment tools.
3. *Electronic Cash System.* E-cash is an electronic or digital form of value storage and value exchange that has limited convertibility into other forms of value and require intermediaries to convert.
4. *Micropayment systems.* Micropayments are financial transactions involving very small sums of money. PayPal is an example of the micropayment system.

From the above mentioned four types of electronic payment systems, the e-payment instruments can be classified into three categories, namely, the pre-paid system, the pay-now system and the pay-later system (Lee et al. 2001):

1. *Pre-Paid System* is comparable to paying in cash. The participant may withdraw an amount of money from user's bank account and store it in an electronic purse, convert it to electronic money, or use a cheque certified by his bank. Examples are E-Cash from DigiCash and cheque from NetCheque (Lee et al. 2001).
2. *Pay-Now System* differs from Pre-Paid system by the fact that withdrawal of money from the bank account is only made at the time of paying.
3. *Pay-Later System* is currently used with credit cards. Money is withdrawn some time after the purchase is made. This system is equivalent to the pay-now system as the buyer sends some sort of form to the vendor in both systems. SET is a common example. Table 3 shows the comparison of three payment models.

Table 3 Evaluation of different payment methods.

	Cash	Cheque	Credit Card
Transaction Cost	Low	Low	High
Consumer Base	Small	Medium	Large
Atomic Exchange	Good	Fair	Poor

Peer-to-Peer Payment	Good	Good	Poor
Anonymity	High	Low	Low

The card payment instrument incurs the highest transaction cost whereas such cost associated with the cash payment instrument is the lowest among the three. This makes the cash payment instrument the best candidate for payment with amount down to charges at the cent level, otherwise the transaction cost would have accounted for a significant percentage over the total amount of payment.

Security of the transaction is the main concern with the electronic payment since money and merchandise are transferred without direct contact between parties involved in the transaction (Laudon and Traver 2002). From the research aspect, Wen et al. (2006) proposed a mobile-agent based distributed e-bank model and its protocols through expanding on Camenisch and Stadler (1993) model (an efficient offline e-cash system based on representation problem). The system modifies the digital signature technique, improves the computation loads and reduces the bandwidth usage. Another secure e-payment subsystem based on Java mobile agent proposed by Li et al. (2001) proposed a secure e-payment subsystem based on Java mobile agent. They carried out the e-payment system using e-money. This subsystem supports anonymity and prevents double spending. However, it only connected to one bank for payment to demonstrate the workability of their model, but further work research work is need to prove the concept in a "multi-banking-finance" mobile agent environment. The design of payment protocols is based on the protocols used in NetCash (Medvinsky and Neuman 1993). The details of the security issues are explained next.

4. Review and Issues of Security, Privacy, Safety and Trustworthiness

Researchers have proposed the use of MAs for e-marketplace trading since 1994. However, its security problems become a major hindrance that limits the usage of mobile agent-based e-marketplace. Herein, we discuss the important issues such as the security issues, privacy, safety and trust issues for MAs when it is applied in the e-marketplace environment.

4.1. Security Issues

Security at the application level covers various aspects including authentication, authorization, message integrity, confidentiality and operational defense (Kannammal and Iyengar 2007). For e-business applications, auditability, non-repudiation and certification are added requirements. In addition, the use of MAs in e-commerce applications would impose other security threats such as eavesdropping, malicious interception, spoofing, uncontrolled cloning, double spending, fraud and audit trail. Thus, security mechanisms will have to be embedded to ensure that MAs will not sacrifice security requirements.

MAs raise a number of security issues. Generally, it concerns two different types of the security problems: one is the protection of platform or host that runs the mobile agent against attacks which can harm or use its resources without permission, another is the essential protection necessary to guard MAs against the malicious hosts that might alter the information it carries when it visits the hosts in its itineraries.

Currently, there are several proposed methods such as sandboxing, authentication, authorization, proof-carrying code, payment check etc. But these methods are not enough to make the e-marketplace fully secured and trustworthy.

The mobility characteristic of mobile agent permits all the required operations to be performed locally in the e-marketplace without maintaining reliable connections with remote hosts and without bandwidth engagement. However, in e-marketplace environment, strong mobility will cause the high-risk security threats.

Generally, mobile agent uses two mobile models: single hop and multi-hop. In e-marketplace environment, multi-hop is more efficient and useful than the single hop. For instance, mobile agent can search for the product in lowest price through the multi-hop to get the message for each node. However, the major weakness for this model is that every visited node may steal the sensitive information (e-cash, credit card number, etc) or change the visited results. Therefore, strong mobility causes high security threats. In contrary, low mobility causes low security threats.

To reduce the security risks of mobile agent, Zhang et al. (2005) proposed a framework for e-commerce that used both single hop and multi-hop to reduce the threaten risk. The first phase uses multi-hop to collect the message. Mobile agent does not take any sensitive information when processing the information collection. The second phase uses single hop to take the sensitive information to reduce the security risks.

4.2. Privacy Issues

It is important to ensure that the information carried by a mobile agent or stored on a platform is accessible only to authorized parties (Kannammal and Iyengar 2007). Privacy is normally handled by encryption. In general, in Public Key Infrastructure (PKI), a message is encrypted and decrypted by public key and privacy key respectively. The public key can be widely distributed, however, only the receiver has the private key. For authentication purposes (proving the identity of the sender, since only the sender has the particular key) the encrypted message is encrypted again but with a private key this time. Cryptography algorithms such as RSA or AES are normally used for encryption in security systems.

Unfortunately, PKI is not an efficient way of sending large amounts of information. It is often used as a first step for two parties to agree upon a key for symmetric secret key encryption. The keys used for the particular message for sender and receiver are generated by a third party: a key distribution center. The keys are not identical, but each is shared with the key distribution center, which allows the message to be read. Then the symmetric keys are encrypted by using RSA algorithm, and rules set under various protocols. Naturally, the private keys have to be kept secret, and most security lapses indeed arise here.

The digital digest uses the hash function and the plain text encrypted with the recipient's public key is sent to the receiver. The receiver decodes the message with their private key and runs the message through the provided hash function so that the message digest value remains unchanged (message has not been tampered with). Very often, the message is also time stamped by a third party agency, which provides non-repudiation.

To address users' concerns over trust and privacy issues, Au et al. (2008) introduced the concept of establishing trust by making use of referrals from external third party in the form of anonymous attribute certificates. Zhao et al. (2007) use the secure message digest and encryption to illustrate the MA-ECM (Mobile Agent-based E-Commerce Model).

4.3. Safety and Trust Issues

The transactions in the e-marketplace require the establishment of a certain level of trust which is responsible for protecting the buyers, sellers and intermediaries from the opportunistic behaviours of other participants in the marketplace (Patel 2010). Trust services are used to verify whether a mobile agent is a legal agent or otherwise through authorization and authentication processes to prevent the existence of malicious agents in e-marketplaces. The trusted third party may be needed as a certificate authority for management and maintenance of keys for encryption purposes, otherwise through authorization and authentication processes to prevent the existence of malicious agents in e-marketplaces.

Safety of a system can be achieved by providing a reliable backup system. This system is used to ensure that transaction data is not lost. Safety should include imposing a maximum limit on the amount of money involved in a single transaction for the users.

Netscape Corporation has developed SSL (Secure Socket Layer) which can be used for information transactions, provides several features including bi-directional authentication between clients and servers, selection of the cryptographic algorithms to use, and handshaking to establish a secure connection.

However, SSL may not be safe for data transmission in mobile agent-based e-marketplace. Thus, another approach altogether is adopted: SET (Secure Electronic Transaction) (Drew 1999). SET uses PKI for privacy, and digital certificates to authenticate participants in e-marketplace. More importantly, sensitive information is not seen by the seller, and is not kept on the seller's server.

To make mobile agent-based systems trusted and safe, Wang et al. (2007) proposed a migration mechanism of security and fault tolerance for mobile agent. In this mechanism, it includes the trust services and travel services. The trust service can be duplicated as backup at several different trusted nodes in the e-marketplace environment. When the trust service expires, the system can select another from the trusted nodes as the trust service is based on an *election algorithm* (Krzyzanowski 2000). However, this mechanism has some drawbacks, such as the expiry of trust services and trusted nodes, which may affect the backup of trust services, therefore causing the travel transmission problem of mobile agent.

5. Review of Auditable and Forensic Services

With the widely increasing use of Web technologies and the Internet over last two decades, many areas (such as information communication technologies, law, social sciences businesses etc.) have become very dependent on these rapidly evolving technologies for social networking purposes. This dependency has opened the opportunities for various types of cybercrimes to take place, where the offenders can commit their acts without being physically present at the crime scenes and leaving few traces, if any (Karyda and Mitrou 2007).

Several common cybercrimes activities to the network are hacking, unauthorized browsing, sniffing and denial of service attacks, also malicious programs that can expose confidential information such as viruses, spyware, worms and Trojans. Therefore, digital forensic, as one of the security measures for safer computing and communications become an intrinsically interdisciplinary field. For example, criminology, law, intrusion detection, forensics and computer science come together to form *digital forensics.* It has emerged as the single most important application for audit functions and cybercrime computer related investigations. It is defined as the process of identifying, preserving, analyzing and presenting digital evidence in a legally accepted manner for the purpose of (McKemmish 1999):

1 *Evidence Identification* is the first step of digital forensic process. Since the digital evidence is required to be presented at the court. The process applied in order to extract and recover the evidence depends on the nature, storage location and format type of the data must be robust.

2 *Evidence Preservation* is the second step of digital forensic process. All the digital evidence should be maintained in a device to ensure that it can be accepted as admissible evidence in a court of law.

3 *Evidence analysis* is the main step in the digital forensic process. It encompasses the extraction, processing and interpretation of data. Since a huge amount of data can be collected and recorded during the forensic examination, analysis of the evidence has become difficult and time consuming. Thus, the forensic tools can be used here to enable the analysis of evidence such as EnCase, Forensic Toolkit and Sleuthkit (James, Whittaker and Howard 2005).

4 *Evidence Presentation.* It is the last step in the digital forensic process. The presentation of digital evidence in a court law aims to prove the illegal activities are real and have ocurred.

From the technical point of view, the major challenge of digital evidence is to establish its authenticity, timeliness and availability. Firstly, hackers always forge their ID when they attacked the systems. They use different types of methods (e.g., viruses, malware and worms) to destroy the attacked evidence. Secondly, it is easy to change the digital crime evidence. Digital forensics investigation can be divided into static evidence and dynamic evidence. The static evidence is collected after the attacks take place. So the difficulty for this type of evidence is determining its authenticity since the information can be altered by the investigators. The dynamic collecting of evidence is based on prior knowledge and assumptions about possible attacks, and if done correctly, it is an efficient way to satisfy cybercrime investigations.

Vicka et al. (2002) defined the dynamic evidence gathering schema for network forensic and produced a network forensic analysis toolkit for real-time evidence investigation. This network forensic tool is primarily of use in the ICT industry to combat cybercrime activities as part of their increasing concern for providing security and protecting against privacy violations. It is used as a network forensic tool to analyse traffic flow information and its contents as and when it happens. However, a more practical approach includes archiving huge quantities of network traffic information and analyzing it either as superset or subsets as necessary when cybercrime or privacy violations are reported. It is easy to monitor the forensic analysis in a network pre-configured mode, but difficult in dynamic changing network configurations based on routing functions and outages. Neverthelesss, the security vulnerabilities and configuration problems can be conveniently identified in either case, with much more analysis work required for dynamic configurations. The network forensic tool can also analyze a complete record of the network traffic with appropriate reconstructive tools to provide context and schemas for other breach-related events for more exact evidence to prosecute. The forensic records allow the investigator to recover lost messages from a database, perform *unhurried* analysis of traffic spikes and application errors to produce more thorough evidence.

A Network Forensic Analysis Tool (NFAT) is a combination of intrusion detection systems and firewall that are used to preserve long term records of all network traffic and allow quick analysis of identified trouble spots. It is an essential compliment to existing security tools. The purpose of the NFAT is to capture the network traffic, analyze traffic according to user's needs and let the system users discover useful and interesting things about the analyzed traffic (Vicka et al. 2002). For the traffic capture, primary concerns for the positioning an NFAT on a network are traffic relevance, data integrity, and packet capture rate. For effective network forensic, an NFAT must maintain a complete record of network traffic. Tcpdump is the most popular capture software. It is useful for collecting traffic when you know the activity of interest is on the wire. To analyze the network traffic, three main stages should be included:

1 *Sessionizing captured traffic.* In first stage, the NFAT organizes data packets into individual transport-layer connections. It allows NFAT to analyze each connection layer by layer of content and protocol. However, unsessioned data is ineffective in this stage.

2 *Protocol parsing and analysis.* In second stage, the system analysis not only looks at the connections but must correlate the connections with each other. The efficient approach is an expert system analysis that allows analysis on each network layer. It gains more power when it goes past the ISO's OSI/RM seven-layer model and into the data stream.

3 *Handling encrypted data.* In the last stage, FTP is an insecure protocol which being replaced by secure cp (SCP), which provides similar functionality (file transfer) within a secure shell. An NFAT can completely encrypt a session. It would allow a file to be transferred fully encrypted and then allow the NFAT to capture, decrypt, and eventually analyze its contents.

Once complete, the analysis of the network traffic is presented through the user interface of the network forensic analysis tool which lists the related records. It is predicted that such tools and mechanisms will not only make be a formidable part of safe e-trading environments but it will also act as a natural deterrent to stop cybercrime.

Carrier and Spafford (2003) introduce the notion of a digital crime scene with its own witnesses, evidence, and events that can be investigated using the same model as a physical crime scene. The proposed model integrates the physical crime scene investigation with the digital crime scene investigation to identify a person who is responsible for the digital activity and applies to both law enforcement and corporate investigations. Wang (2006) mentioned that as computer networks, internet systems and software development become integrated with the digital forensic and forensics tools, forensics plays an important role for the system that makes the system more secure and trustworthy.

In an e-marketplace environment, real time digital forensics framework includes several components such as data collection, data analyzing, and protocols, identify digital forensics, report the digital evidence, etc. We can use the static agent and mobile agent to carry out these components to improve the intelligence, self-adaptability, flexibility and fault-tolerance in distributed network for digital forensics. Using mobile agents to represent the digital forensics can automatically collect the network data from multiple mobile agents and servers in a distributed heterogeneous system. This can reduce the data storage requirements of a single monolithic system; reduce the bandwidth and communication overheads. As a dynamic forensic model that employs the mobile agent mentioned by Wang et al. (2007), the model uses the analogy of the biological cell immunity theory. It relies on collecting real-time network intrusion evidence dynamically, and saving it in a secure location, for later use by forensics investigations. The system has three components:

1 *Detector Agent* captures real-time data from the network, and it uses a code matching mechanism to determine an intrusion behavior. A forensic request is sent in a request message to a Forensic Agent.

2 *Forensic Agent* collects digital evidence by capturing snapshots from host and network to generate original evidence.

3 *Response Agent* analyzes captured evidential information and replays the attacking procedure.

By using the digital forensic tools such as NFAT, the packets can be re-organized into individual transport layer connections between machines, resulting in more forensics details.

In computer networks there are various mechanisms, devices, software, and protocols which are interrelated and integrated. The rights of an internet user acting anonymously conflicts with the rights of a server victim identifying the malicious user has to be resolved. Antoniou et al. (2008) proposed a security protocol called ERPINA protocol for privacy

and forensics investigation process which dramatically increase the level of the protocol's reliability. The ERPINA protocol addresses the reliability issue efficiently by defining what is considered as malicious and what is not at the beginning of a communication. This model also has been partially used in the research work reported by Jailani et al (2008). The ERPINA protocol supports digital forensic functions is divided into three phases:

1 The goals of the initialization phase are to establish a relation between directory service, anonymous user and a forensic trouble ticket to provide a common security policy for server and anonymous user to agree with and establish the responsible entity corresponding to the need of a server to reveal the identity of a potential attacker.

2 The main phase serves the need of the anonymous user to exchange confidential messages with the server using secret keys. The actual communication takes place in this phase.

3 The goal of forensic investigation phase is to collect evidence and reveal the identity of the attacker to the server, in case the user is indeed an attacker.

Computers in the e-marketplace environment carry out auditing processes. This is not the same as in the traditional auditing which requires all information to be stored in a database or hard drive as the digital evidence. Thus, the authenticity of the audited evidence for the business activities depends on the security, reliability and accuracy of the network. To reduce and control the risks involved in auditing, digital forensic should be used. To make the audit service more secure, more investigation on certificate authority, e-bank or e-cash, cryptography techniques, etc should be carried out.

The audit and forensic technologies have been recently applied in e-marketplace system development. For example, Jailani et al. (2008) and Patel (2010) describe the digital forensics investigation and audit scenario for the agent-based e-marketplace. The scenario portrays a malicious anonymous user attempting to abuse the e-marketplace environment. The concept can be used to detect attacks in such an environment. A model of computer dynamic forensics for e-marketplace designed by Hao and Liu (2006) described the problems of the dynamic forensic such as the reliability and integrity. The model uses the remote server to collect the real-time information. It is then transfers the collected data to the database for analyzing after data filtering. The digital evidence will be recorded at the forensic database when the analyzing is completed. The model uses SSL-based cryptography and authentication mechanism to protect the confidentiality of the information.

6. Research Direction and Discussion

From what has been set out above, the current mobile agent-based framework and systems have their weaknesses especially from security point of view. Most researchers focus on these issues specifically in the area of privacy, trustworthy and safety, and less attention has been paid on the requirements of digital forensics of transactions that happen in e-marketplaces. This is the area that we should be concerned with when developing a mobile agent-based e-marketplace system.

Future research would be to propose a mobile agent-based framework standard and develop a working system prototype which is based on the initial concepts that were proposed by Jailani et al. (2008) and extended by Patel (2010) that would address the issues of security, trust, safety, privacy, and digital forensics as a mandatory part of an e-marketplace framework. There are several security protocols that need to be defined in the proposed framework such as SET and other e-secure-payment protocols for negotiation, mobile agent transmission, digital forensics, and so on. These requirements could be defined and specified using a formal model such as UML to illustrate the functional architecture.

A prototype system based on these concepts has been developed by the authors to demonstrate that the proposed framework is feasible. For implementation, Java-based technologies Mobile Agent System (MAS) i.e. Aglets, J2EE for Web-based system have been used to realize this prototype e-marketplace system with XML and other security components such as the SET and the cryptography techniques to make up the e-secure-payment component. The experiment will be conducted through the comparison between the proposed system and MA-ECM (2005).

6.1. Broader Research Challenges

Other than technical requirements, there are several areas that both de facto and de jure regulatory and standards'

bodies, governments and industry will have to address as part of a comprehensive MAS deployment strategy in the wake of new methods and applications of e-business and e-trading. The important ones among the non-technical and technical ones are:

1 *Safety measures* (encompassing audit, digital forensics, privacy, protection, security and trusted computing) policy management defining a framework to synthesize legislations, directives and guideline in a formal design language is deemed essential to have provable technical solutions. Can automatic rule-based policy management tools be used to generate and select a set of prescribed safety measures against a mandate for MAs? Yes. Such a language should feed into the MAS/MA software development life-cycle to engineer rapid product creation and deployment. IBM's EPAL (2003) is an example in that direction. A comprehensive language is needed to build fully-fledged MASs.

2 *Privacy* needs to be simplified for end-users to understand and use. The selection from given profiles is not easy even for those persons having ICT background, so how should a novice understand it? New "aiding and abetting" models and supporting techniques are needed that can "perceive" end-user's requirement for privacy through usage and seamless profile building and coercing the user to engage in protecting him/herself. Besides this, privacy functions have to be tied to digital forensics and audit on the one side for law enforcement and infringement prevention purposes and on the other side if it is to achieve higher levels of privacy for its end-users.

3 *Security* issues that need to be resolved for the deployment of advanced intelligent MAs should include measures for non-mutilation of messages to avoid disturbance and miscommunication across a range of technologies, network types and applications within the MAS environment. Privacy for non-disclosure of personal data in messages between MAs will have to encrypt/decrypt without the knowledge of end-users to ensure ambient access and seamless Web access and Internet surfing. Many advanced non-repudiation techniques will have to be derived and developed to avoid denial of messages being sent when exercising legal rights and for digital forensic purposes. The understanding of MAs to perform in this mode of operation is very challenging at the present time.

4 *E-payment* security measures will have to go further and be more robust than they are today to avoid the kinds of fraud that are prevalent on the Internet. Integrated e-payment schemes will have to be defined for global e-trading operations crossing many jurisdictions and MAS made to operate with complete audit trails and non-repudiation facilities. It is perceived that new international e-trading norms, agreements and laws are essential if the e-business environment is to open up and be trusted. It is also expected that in the future MAs will have to pay for services consumed and resources used at remote locations on a metered unit basis in this global MAS environment. This becomes a new requirement on accounting management to ensure that taxes, duties and other dues will be paid to the relevant authorities in a global economy context. It needs new MAS paradigms to be defined.

5 *Management* issues of MAS are very complex indeed. They bring together many techniques and technologies offering new forms of e-businesses that span many enterprise processes and business models which require new management policies, strategies, methods and models. MAS management should be automated against a variety of profiles defining *e-everything*. The MAS area is ripe for taking onboard autonomic computing principles for management functions to become collaborative, cooperative self-determining, self-opportunistic, self-diagnosing, self-monitoring and self-healing against profiles generating rule-based policy models and structures. At present, hardly any Research and Development (R&D) work has been done in this area, but the authors are convinced that a host of new challenges await the unsuspected minds.

These topics together with those presented elsewhere in this paper regarding MAS and their MAs in the area of mobile technology for e-business present very challenging research and development opportunities and potential pay-offs.

7. Conclusion

This paper reviewed and investigated the current state-of-the-art in the design and implementation of a framework and systems for secure, trusted and auditable mobile agent-based e-marketplace trading. It vividly gave an analysis of existing

mobile agent-based e-marketplace frameworks and systems. It presented the potential dangers and critical issues of using mobile agent technologies in e-marketplace environments. It listed and described the broad range of security requirements for mobile agent-based e-marketplace infrastructure services and the e-payment systems, followed by reviewing the issues of the security, privacy, trustworthy and safety aspects for making safe e-trading possible in an e-marketplace as a composite function. It then elaborated upon the reasons, the need and methods for auditable and forensic services for e-marketplace to be included in any framework and ensuing systems to not only investigate against cybercrime but also to protect and deter against cybercrime activities.

Currently a prototype is being developed to assess the functional behavior and computational aspects of the system and validate and verify the digital forensics protocols of the mobile agent-based e-marketplace environment in the context of secure trading and payment. From this exercise we plan to define the trust model for safe e-marketplace in an open e-trading environment. We are also investigating the use of smart intrusion detection and prevention systems based on autonomic computing and some recent developments from the subject fields of artificial intelligence and data mining.

In our future research work, we will continue to investigate the computational effectiveness of mobile agent-based e-marketplace as well as exploring the appropriate techniques to support secure, trusted, reliable, effective and auditable transactions.

References

Alfalayleh, M., and Brankovic, L. 2004. An Overview of Security Issues and Techniques. *In Mobile Agents, Proceedings of the Eighth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security* (CMS2004). Volume 175, pp. 59-78.

Antoniou, G., Leon, S., Stefanos, G., and Paramalli, U. 2008. Privacy and forensics investigation process: The ERPINA Protocol. *Journal of Computer Science & Interface.* Vol 30, Issue 4, pp. 229-236.

Anderson, M.M. 1998. Electronic Cheque Architecture, Tech. Rep. Version 1.0.2. *Financial Services Technology Consortium.*

Bakos, Y. 1998. The emerging role of electronic marketplaces on the Internet, Communications of the ACM 41 (8) pp. 35-42.

Brands, S. 1993. An efficient off-line electronic cash system based on the representation problem, Technical Report CS-R9323, CWI.

Carrier, B., and Spafford, E.H. 2003. Getting Physical with the Digital Investigation Process, *International Journal of Digital Evidence,* Fall 2003, Vol 2, Issue 2. pp. 20

Chen, N.J., Huang, S.Z., and Su, D.F. 2000. Research on Applied Technology of Mobile Agent in Electronic Business, J*ournal of Information Technology & Informatization*, Vol 2. No. 12. pp. 48-50.

Dasgupta, P., Narasimhan, N., Moser, L. E., and Melliar-Smith, P. M. 1998. A Supplier-Driven Electronic Marketplace using Mobile Agents. *Proceedings of the 1st International Conference on Telecommunications and Electronic Commerce*, Nashville, USA, pp. 42-50.

Drew, G.N. 1999. Using SET for Secure Electronic Commerce, Prentice-Hall, Inc. New Jersey. pp. 265. ISBN:0-13-099715-3

Ghenniwa, H. H., and Huhns, M. N. 2005. An Agent-Oriented Marketplace Architecture for Enterprise Integration, *in the Encyclopedia of Information Science and Technology*, M. Khosrow-Pour (Ed.) , Vol I-V, pp. 1899-1905.

Jailani, N., Yatim, N.F.M., Yahya,Y., Patel, A., and Othman, M. 2008. Secure and auditable agent-based e-marketplace framework for mobile users. *Journal of Computer Science & Interface.* Vol 30, Issue 4, pp. 237-252.

Jailani, Norleyza, Ahmed Patel, Muriati Mukhtar, Salha Abdullah and Yazrina Yahya 2010. Concept of Mobile Agent-based Electronic Marketplace. In *Encyclopedia of E-Business Development and Management in the Digital Economy.* Edited by I-Lee, by IGI Global publications. Publisher: Business Science Reference. ISBN: 978-1-61520-611-7 Release Date: February 2010.

James A., Whittaker J.A., and Howard, M. 2005. Computer Forensics. On-line IEEE Security and Privacy. http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html (accessed September 2, 2009)

Hao, G.Y., and Liu, F. 2006. Research on Computer Dynamic Forensic in E-marketplace Environment. Market Modernization. Vol. 32, No. 15. pp.126-128.

IBM Aglet Workbench [EB/OL]. 2004. http://www.trl.ibm.co.jp/aglets/. (accessed August 12, 2009).

IBM. Enterprise Privacy Authorization Language (EPAL), Version 1.2, 2003 submitted to the W3C. http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/. (accessed June 15, 2009).

Kannammal, A., and Iyengar, N.Ch.S.N. 2007. A Model for Mobile Agent Security in E-Business Applications. International Journal of Business and Information. Vol 2. No. 2. pp. 185-198.

Karyda, M., and Mitrou, L. 2007. Internet Forensics: Legal and Technical Issues. *Second International Workshop on Digital Forensics and Incident Analysis* (WDFIA 2007). pp. 3-12. ISBN:0-7695-2941-0.

Krzyzanowski, P. 2000. Process Synchronization and Election Algorithms. Lectures note on distributed systems. from http://www.cs.rutgers.edu/~pxk/rutgers/notes/content/06- mutex.pdf (accessed October 16, 2008)

Laudon, C. Kenneth and Traver, Carol. 2002. E-commerce: Business, Technology, Society, New Delhi: Pearson Education. No. Page, 800. ISBN: 0201748150

Lee, T.O., Yip, Y.L., Tsang, C.M., and Ng, K.W. 2001. An Agent-based Micropayment System for E-Commerce. in J. Liu and Y. Ye, ed. E-Commerce Agents. Lecture Notes in Artificial Intelligence vol. 2033 (Springer-Verlage Berlin Heidelberg). pp. 247-263.

Li X., Lu, J., Cao, C., Feng, Y.X., and Tao, X.P. 2001. Research on the Security of Mobile Agent-based System, *Journal of Software,* Vol13, No.10. pp. 1991-2000.

Mahmoud, Q. H., and Yu, L. 2006. Making Software Agents User-Friendly. Computer, Vol. 39, No. 7, pp. 96, 94-95, doi:10.1109/MC.2006.239

McKemmish R. 1999. Trends and Issues in crime and criminal justice. *Australian Institute of Criminology*. No. 118. pp. 37-47.

Medvinsky G., and Neuman, B.C. 1993. Netcash: a design for practical electronic currency on the internet, In: ACM SIGSAC. pp. 1026-106.

Patel, A. 2010. Concept of Mobile Agent-based Electronic Marketplace – Safety Measure. In *Encyclopedia of E-Business Development and Management in the Digital Economy.* Edited by I-Lee, by IGI Global publications. Publisher: Business Science Reference. ISBN: 978-1-61520-611-7**,** pp. 252-264 in volume 1**.** Release Date: February 2010.

Rivest, R., Shamir, A., and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM,* 21 (2), pp. 120-126.

Song, R., and Korba, L. 2003. Security Communication Architecture for Mobile Agents and E-commerce, in *Proceedings of the 2003 International Work shop on Mobile Systems, E-Commerce and Agent Technology* (MSEAT'2003), Miami, Florida, USA.

Vicka, C., Charles, P., Sybil, S., Greenbergichael S., and Van B.J. 2002. Network Forensics Analysis, *IEEE Computer Society*, 6(6): pp 60-66.

Wang, D.G., Li, T., and Liu, S. 2007. Dynamic Network Forensics Based on Immune Agent. *Journal of Wuhan University: Natural Science Edition*, Vol. 52, No. 5, pp. 527-531.

Wang, R.Y., Liang, L., and Liu, W.F. 2004. Research of Mobile Agent- based Security in the E-commerce, *Journal of Application Research of Computers.* Vol. 11. No. 8. pp.137-138.

Wang, Y., Wang Z.Q., and Wei, L.F. 2007. A Migration Mechanism of Mobile Agent System Supporting Security and Fault-Tolerance. *Journal of Computer Technology and Development*, Vol. 17, No.3. pp. 169-175.

Wang, Y.Q. 2006. Computer Forensics Technology of Criminal Activities in Communication Networks. *Journal of Telecommunications Science.* Vol. 22, No 6. pp.63-66.

Wen, T., Wang, J.Y., and Liu, J.R. 2004. A model and its Protocols of Distributed Electronic Bank Based on Mobile Agent, *Journal of Mini-Micro Systems.* Vol. 24, No.3. pp. 331-335.

Yu, B., and Li, X. 2006. Mobile Agent-based Encryption Transmission System. National Computer System Software Annual Meeting. pp. 24-34.

Zhou, K.J. 2007. Mobile Agent-based Cooperative E-commerce Security Authentication Mechanism. *Journal of Computer Engineering,* Vol.33, No.9. pp.171-173.

Zhang D.L, and Lin, C. 2005. Security Model of Mobile Agent in E-commerce. China Academic Journal Electronic Publishing House. Vol. 25. No.6. pp. 1271-1273.

Zhao, S.H., Xin, F.Q., and Ma, J.Z. 2007. Research on Secure Mobile agent-based Electronic Commerce. *Journal of Science and Technology Information.* Vol. 2. pp.10-11.