Agent Based Secured e-Shopping Using Elliptic Curve Cryptography

Sougata Khatua[*1], Arijit Das [2], Zhang Yuheng [3], LI Li [4] and N. Ch. S. N. Iyengar [5]

*SCSE, VIT University, Vellore-632014, Tamil Nadu, INDIA[*1]*
International School of Software, Wuhan University, Wuhan, China [4]

sougatakhatua@yahoo.com[*1], arijitdasmid@yahoo.com [2],*
yuer.zhang1987@gmail.com [3], lli@whu.edu.cn [4]
and nchsniyengar48@gmail.com [5]

Abstract

e-shopping has grown in popularity over the years, mainly because people find it convenient and easy to buy various items comfortably from their office or home. This paper has proposed a personalized e-shopping system, which makes use of agent technology to enhance the automation and efficiency of shopping process in Internet commerce. The agent technology is used to enhance the customer's needs which include availability, speedy response time, and efficiency. Agent for e-Shopping creates connectivity on an anytime-anywhere-any-device-basis to provide the specific goods required by the consumers. But Internet being heterogeneous and non secure medium; privacy, authenticity, integrity, and non-repudiation are the key requirements to be addressed by such systems where face to face interaction is not possible. Most of the systems do not provide the required level of security service so that many problems exist in the systems like denying, losing, misusing, stealing double-spending etc. This paper address all the above said security service problems to an e-shopping system using Elliptic Curve Cryptosystem (ECC).

Keywords: *JADE, client agent, controller agent, Encryption process, Decryption process, digital signature, confidentiality, integrity, non-repudiation, authentication.*

1. Introduction

The e-shopping is defined as the use of computers and electronic networks to organize shopping with customers over the internet or any other electronic network.

Online shopping has grown in popularity over the years, mainly because people find it convenient and easy to buy various items comfortably from their office or home. One of the most advantages of online shopping, particularly during a holiday season, is that it eliminates the need to wait in long lines or search from store to store for a particular item.

The unpredictable growth of the Internet users in world opened a new business opportunity to the whole world. Shopping activities over the internet have been growing in an exponential manner over the last few years. One of such environments in which there is a prominent job for the agents would be e-shopping in which a user is able to give those agents the responsibility of buying and selling, instead of searching the e-shopping himself [10]. There are no proper mechanisms to facilitate electronic transaction and automate shopping process on behalf of customers. So a human buyer is still responsible for gathering commodity information from multiple suppliers on Internet, making decisions about each commodity, then making the best possible selection, and ultimately performing the e-payment. So it takes

lot of time to buy things over the Internet [6]. Hence, to reduce the time and to enhance the automation of the e-shopping system a multi agent environment is used.

But Security is often sited as a major barrier to further development of e-shopping on the open Internet [7], such as clients' information divulging, credit card embezzling, and so on. These problems warn people in e-shopping and make them reluctant to pay on Internet. Therefore, the most important topic is how to establish a secure and well-suited applied condition to provide adequate protection to the related transaction information for each entity in an e-shopping transaction.

1.1 Security Features

The main concept of security of the e-shopping is defined below:

Confidentiality: The shopping information in the transaction all demand for secrecy. For instance, all the things such as, credit number, total amount of shopping and the user name & password can't be known about by anybody else. Therefore, it is generally required to be encrypted in the process of information dissemination.

Integrity: It is classified into the following categories [2]:

i) Integrity of Transaction: when the money is sent from customer to the supplier the integrity of the transaction must be maintained i.e. debit and credit of amount must not changed. Failure to this will lead to an inconsistence state which is highly undesirable.

ii) Delivery of Product: The customer must receive the product in good condition. It is undesirable that customer pay the money without receiving the product.

Authentication: It ensures that the people using the computer are the authorized users of that system before transacting.

Non-Repudiation [3]: It ensures that neither the customer nor the supplier can deny communication or other action regarding information or resources at a specific time.

i) Non-repudiation of origin: The ability to identify who sent the information originally versus which intermediary forwarded it.

ii) Non-repudiation of receipt: The ability to identify that the information was received by the final addressed destination in a manner that cannot be repudiated.

iii) Non-repudiation of delivery: The ability to identify whether the information was delivered to an appropriate intermediary in a manner if cannot repudiate.

Availability: It ensures that end system (host) and data should be available when needed by the authorized user.

Accountability: The identities of all users are assured and are made responsible for their action [20].

Copy Protection: This feature ensures protection from unauthorized copying of intellectual information [8].

2. Background

The security of the e-shopping system is based on the following components of the cryptography:

Public Key Cryptosystem (PKC): i.e. for encryption and decryption of the confidential information such as credit card/debit card number. Both *Secure Socket Layer (SSL)* and *Public Key Infrastructure (PKI)* are based on PKC.

Digital Signature: This is used to provide integrity of the information like payment amount, authenticity of the user and availability of the information to the authenticated user.

Password Based Authentication: It is used to check the user identity. It is the simplest and oldest method of entity authentication.

Agent Technology [1]: An agent is a self-directed and identifiable entity that performs one or several tasks in order to achieve some goals. In networking, an agent can run even if the user disconnects from the network. During the agent lifetime, an agent could migrate from an execution environment to another. The agent migration process consists of deactivating the agent, capturing its state, transporting the agent to a new location, restoring the agent state, and resuming the agent execution.

The different types of agent platforms have been developed: AGLETS, JADE, VOYAGER, TACOMA, GRASSHOPPER, and SPRINGS.

2.1 Comparison of Mobile Agent Platforms

We compare the above agents' platforms on major features which can affect their applicability as shown in Table 1. In the table we evaluate the following characteristics of each platform.

1) *Security:* Strong security mechanisms are desirable in technologies operating in heterogeneous distributed environments like World Wide Web. Security protects agents against host and from other agents.
2) *Communication Technique:* Communication notifies the agents to handle incoming messages from other agents. Asynchronous communication is more efficient as compared to synchronous communication.
3) *Mobility:* Mobility can reduce network traffic and can increase efficiency of agents.
4) Whether it supports graphics based tools or not.
5) The platform supports different operating systems and languages.

Table 1: Comparison of Mobile Agent Platforms

Agent Platforms → / Features ↓	Aglets	JADE	Voyager	TACOMA	Grasshopper	SPRINGS
Security	Limited	Strong	Limited & Secured Channel	Uses firewall agent	Limited	Limited
Communication technique	Synchronous, Asynchronous	Asynchronous	All methods	Asynchronous	Synchronous	Synchronous, Asynchronous

Mobility	Aglet transfer Protocol	In-built agent mobility service	Java object Series	Transfer control Protocol	Dynamic proxies(region server)	Dynamic proxies (location wise)
GUI Based Tools	Some	Yes	No	Some	Yes	No
Operating system used	JDK 1.1.x on Win32, OS/ 2 Warp Version 3 and 4, AIX 4.x, Solaris for SPARC.	All (with JRE)	UNIX, Linux Windows	Unix,Win95, Win NT, PDA systems	WinNT/ 9x, Solaris Should run on all platforms supporting JDK 1.1	Linux
Programming languages used	JAVA 1.1	JAVA 1.1	JAVA 1.1	C, Perl, Unix, Tcl scripting language	JAVA 1.1	JAVA 1.1,1.2
Organization	IBM Tokyo Research	Telecom Italia Lab	Object space	Tromoso and Cornell University	IKV++	Distributed Information Systems Group

This study analyzed six agents' platforms developed by different groups. On comparison JADE, mobile agent platform seems most appealing. It is the platform which is purely designed in Java and supports different kinds of devices operating in internet. It provides strong security mechanism and supports agent mobility.

3. Literature Review

There are so many works related to the project available in the literature. Some of them are discussed.

3.1 Previous Works

Software agent technologies provide a new scenario that is used to develop the new-generation e-commerce system, in which the most time-consuming stages of the customer's shopping process will be automated [15].

Moreover, there are now many different shopping sites on the Internet; however, most of these sites lack a user-friendly interface design, which is essential for the success of online software [10]. The interface of e-shopping systems must be pleasing to the eye, effortless to learn and easy to use [5]. Otherwise, people in general will likely become less interested in e-shopping applications. The JADE technology can be used because JADE is completely written in JAVA and can be used [13] to build a user friendly, easy to learn and pleasant.

Amazon, a well known online book seller, uses web based application which is relatively slow and less efficient because it has the following disadvantages [7]:

1. It requires user's direct interventions.
2. It is time consuming.
3. Product comparison is difficult.

Besides these, the web based applications are difficult to scale [9], but the agent based applications are very easy to scale.

In e-shopping, the concerns about security are increasing dramatically [18]. Though a great technical development have been experienced, security incidents continue to occur. To provide the security in several sectors of e-commerce including e-shopping, several research work has been done.

Some *e-commerce* applications (including *e-shopping*) use *Elgamal* cryptosystem. But it also suffers from large key size (1024 bits) to achieve the required level security. In another research paper [2], *PKI* technology is proposed for security in *e-commerce*. *SSL* [3] is used in many e-commerce applications but it also suffers from the problem of large key size because *SSL* depends on *RSA* encryption for exchange of the session key and client/server authentication. But it is too tricky to use the key of 1024 digit and it is relatively slow for this large key size. However, the *RSA* itself is vulnerable [8]. A research work has suggested to use XML encryption [4] with the certain technologies for better security. But the drawback of this technique is that only XML files can be used.

3.2 Proposed Work

To address all the above said disadvantages and security concerns, the JADE technology and the Elliptic Curve Cryptography is used in this project. Using the JADE technology, all the disadvantages of the existing e-shopping systems can be overcome.

The JADE framework facilitates the development of complete agent-based applications by means of a run-time environment implementing the life-cycle support features required by agents, the core logic of agents themselves, and a rich suite of graphical tools. As JADE is written completely in Java, it benefits from the huge set of language features and third-party libraries on offer, and thus offers a rich set of programming abstractions allowing developers to construct JADE multi-agent systems with relatively minimal expertise in agent theory. JADE was initially developed by the Research & Development department of Telecom Italia s.p.a [11].

The JADE agent has the following advantages:

- **Agent is Autonomous:** The JADE agent is Autonomous. The each of the agent have own thread of execution and they can control own life-cycle and decide autonomous when to perform which actions.
- **The system is peer-to-peer:** Each agent can be identified by global name, and using the name they can join and leave a host platform any time. They also can discover other agents through both white-page and yellow-page services.
- **Is fully distributed system:** The each of the agent running as a separate thread. They can run in different machines, and also can communicate between them.
- **A library of interaction protocols:** They already give some of the protocol option in the JADE library.
- **Support for J2SE, J2EE, J2ME** platform and wireless environment.
- **Platform independent:** It can be used in any operating system.
- **Security:** It has strong security features.

Using the JADE agent technology, the proposed e-shopping system has the following characteristics [14]:

1. **Autonomy:** The system has the autonomous transaction facility. It reduces the user intervention during purchasing activity.
2. **User adaptability:** The user preference changes all the time. The system reflects the user's up to date preferences in an adaption mechanism.
3. **Multiple store server access:** It compares the price at different shopping systems and provides the best price for the commodity product chosen by the customer.
4. **Scalability:** Using JADE technology, the system can easily scale up to 1500 agents and 300000 ACL messages.
5. **Faster:** The proposed e-shopping system is faster than the existing systems.

To overcome the security drawbacks of the existing e-shopping system which mostly uses *RSA* and *Elgamal* cryptosystem for providing security, in this project we emphasize on the *Elliptic Curve Cryptosystem* (ECC) as an alternative to *RSA* and *Elgamal* cryptosystem. ECC was first proposed by Miller (1986) and Koblitz (1987), and its security was based upon the difficulty of elliptic curve discrete logarithm problem (ECDLP).

3.2.1 Why ECC:

1. Faster than any other public key cryptosystem.
2. Low power consumption.
3. Low memory usage.
4. Low CPU utilization.
5. Less data traffic.
6. ECDLP is harder than both integer factorization problem and discrete logarithm problem modulo p.
7. Less key size (160 bit) needed compared to *RSA* and *Elgamal* (both needs 1024 bit key) to achieve the required level of security.

Encrypted password: For password based *authentication*, we emphasize to use *encrypted password* using ECC to make almost impossible for the attacker to guess the password.

Besides these, a new key pair (private key and public key) is generated every the system is run. That means a new key pair is generated for each session to make almost impossible to do any type of forgery.

4. Design Analysis

The design of the e-shopping system is divided into two parts:

Internal Design: Here, the internal structure of the e-shopping system is shown and also how the work is going on internally is illustrated.

External Design: Here, the external components are shown and also hoe they work and communicates using message passing are illustrated.

4.1 External Design

Architectural Diagram: It describes the overall design of the system how it works and what are the functional components and what is their functionality.

Sequence Flow Diagram: It shows how the how the components of the e-shopping communicate with each other the messages with respect to time.

4.1.1 Architectural Diagram:

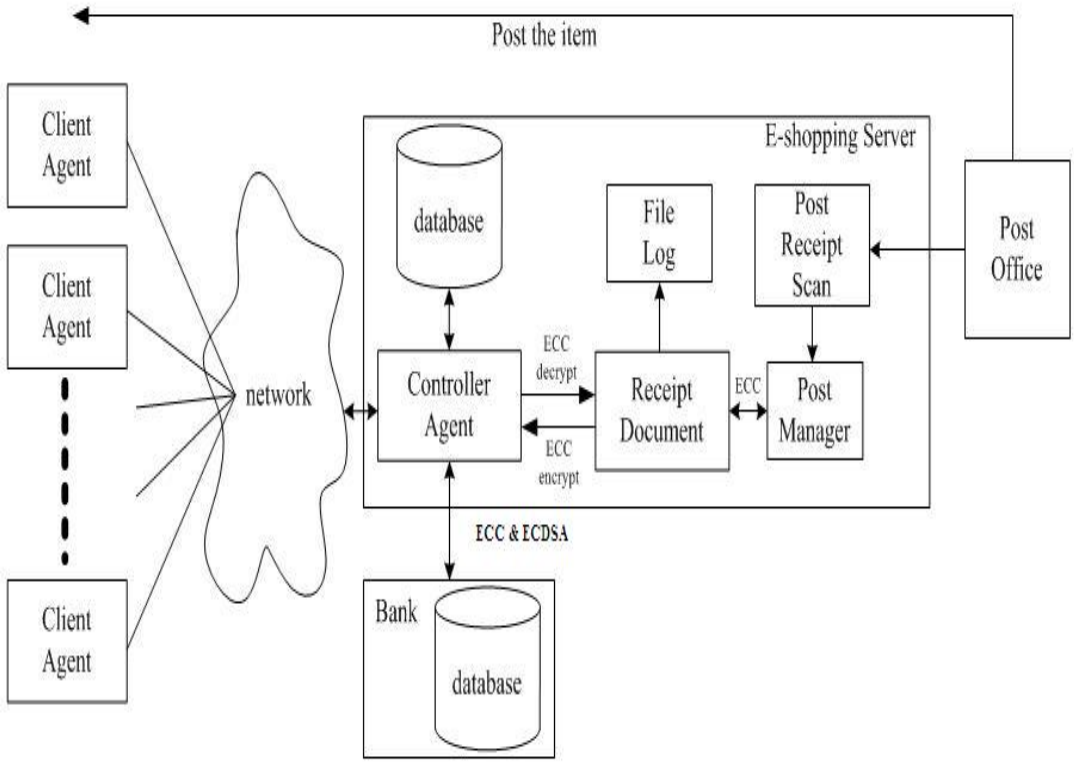

Figure 1: Architectural Diagram of an Agent Based Secured e-Shopping System using Elliptic Curve Cryptography

4.1.1.1 Functional Components and their Functionalities

Client Agent (CA): When the customer logs in to the e-shopping system, the customer must prove his/her authenticity to the system. The Client Agent (CA) takes the username and password of the customer and sends it to the Controller Agent (CTA), if these are correct, then only the customer can enter into the e-shopping system. After that the CA show different items available in various shops in the e-shopping system. The customer can choose at most 9 items from any shop. After putting items into the shopping cart, the customer enters the credit card number and password which is encrypted with Elliptic Curve Cryptography (ECC). These two information are checked by the Controller Agent (CTA) and produces a receipt if the credit card number and the password provided by the customer are correct.

System Server: The system server stores all the information into a database. The system server does not perform the task of checking user name and password and the credit card information. It only stores all those information. If the credit card information is correct, then it passes it to the merchant bank.

Controller Agent (CTA): The controller agent (CTA) performs the entire task on behalf of the system server. It supplies the commodity information or the item details to the Client Agent (CA) according to the customer demand. It also helps the system server to store the customer details in to the system server's database. It encrypts and signs the credit card information using ECC and ECDSA and then, sends to the merchant bank and produces the encrypted and signed receipt document using ECC and ECDSA for the post manager. Besides these, one of the main function of the CTA is the capability to kill a Client Agent (CA).

Database Server: The database server stores all the data. It stores the following information:

- The user information.
- The username and password of the customer.
- The credit card number information.
- The commodity or the item details available for shopping in the shopping system.

Merchant Bank: The bank which has a business relationship with the e-shopping system receives the data from the e-shopping system. This type of transaction is called as business to business transaction. The merchant bank first checks, if the customer is the user of this bank or not. If the customer is a user of this bank, then it transfers the money from customer's account to the e-shopping system's account. If the customer is not a user of this bank, then the data sent by the e-shopping is sent to the customer's bank.

Customer's Bank: It receives the data from the merchant bank. This type of transaction is called as business to consumer transaction. The merchant bank first checks, if the customer is the user of this bank or not. If the customer is a user of this bank, then it decrypts and verifies the confidential information using ECC and ECDSA and then, transfers the money from customer's account to the merchant bank and the money is credited to the e-shopping system's account in the merchant bank.

Post Manager: The post manager receives the encrypted and signed the receipt document using ECC and ECDSA from the Controller Agent (CTA) and then decrypts and verifies it. If the verification is successful, then it decrypts it and posts the brought commodity items through the post office.

After that the merchant bank sends an approval message to the e-shopping system and then the e-shopping system verifies the delivery address and then sends a confirmation to the customer.

The confirmation message is in the form of a number which is called as "receipt number". The receipt number is unique for each shopping. This number is generated only after the successfully completion of the transaction.

The customer should keep the receipt number so that he/she can verify the receipt number at the time of delivery of the items which he/she has brought.

4.1.2 Sequence Diagram

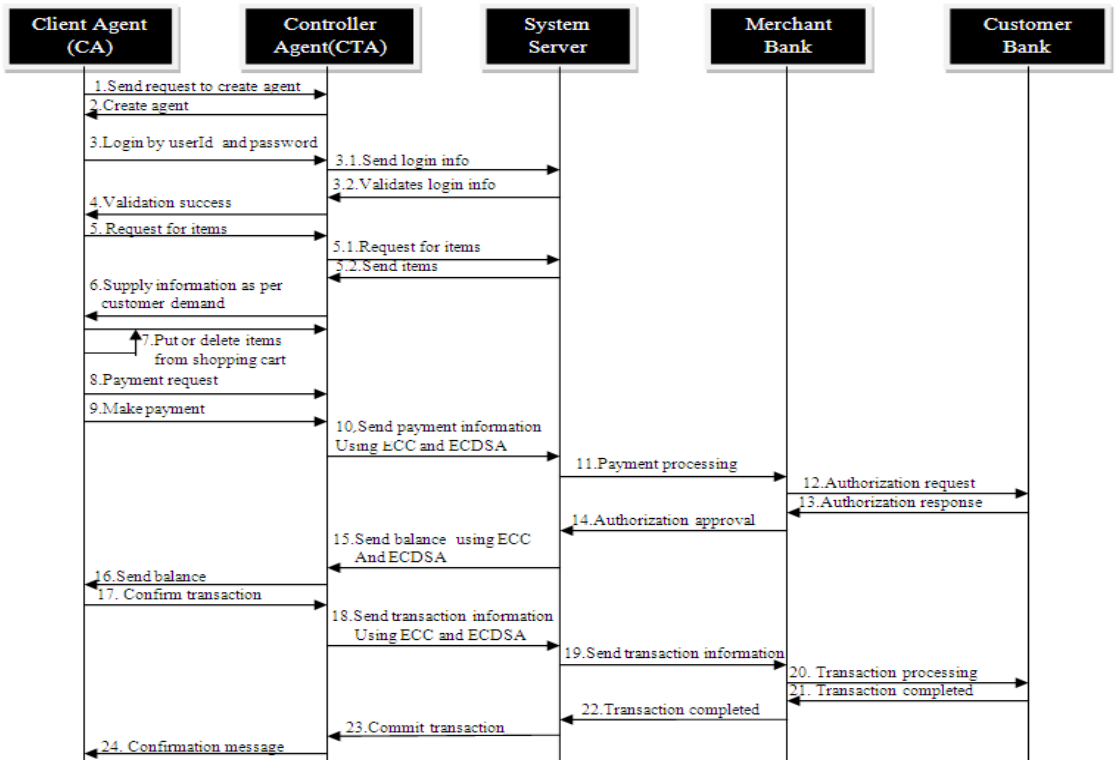

Figure 2: Information Flows for Transactions using ECC and ECDSA

As illustrated in Figure 2, following are the steps:

1. At first the Client Agent (CA) sends request to the Controller Agent (CTA) to create the CA.
2. After that the CTA creates the Client Agent (CA).
3. Then, the customer login to the system by providing userID and password through the CA and CA passes this information to the CTA .
    - CTA passes this information to the system server.
    - The system server sends the validation information to the CTA
4. The e-shopping system returns validation success to the CTA if the customer is an authenticated user of the e-shopping system and the customer enters into the e-shopping system.
5. After that the CA requests to the Controller Agent (CTA) for commodity items.
    - Then the CTA requests for the commodity items to the system server.
    - After getting the message, the system server sends the commodity items to the CTA as per customer demand.
6. Then the CTA receives the information from the system server and supply this information to the CA which displays this information to the customer.

7. The customer selects items and put into the shopping cart or deletes items as he/she wishes.
8. The CA make payment request on behalf of the customer to the CTA.
9. Then the CA makes payment and sends this information to the CTA.
10. After receiving this information, the CTA sends this encrypted and signed information using ECC and ECDSA to the system server.
11. After getting the customer's details, the shopping system (merchant) it contacts to the merchant bank for customer authorization and payment.
12. Merchant's bank will contact to the customer's bank and send authorization request.
13. The customer first decrypts and verifies the information using ECC and ECDSA. If the customer is authorized, then customer's bank will send authorization response to the merchant's bank.
14. Merchant's bank i.e. the e-shopping system's bank will send authorization approval to the e-shopping system.
15. Then the system server sends the balance information to the CTA.
16. After getting the balance information from the system server, the CTA encrypts and signs using ECC and ECDSA respectively and forwards it to the CA and CA displays it to the customer.
17. The customer then sends the transaction through the Client Agent (CA).
18. After, that CTA encrypts and signs using ECC and ECDSA respectively, and sends the transaction information to the system server.
19. After receiving the transaction information from the CTA, the system server sends it to the merchant bank.
20. Then, the merchant bank sends it to the customer bank and it processes the transaction.
21. When, the transaction successfully completed, it sends a message to the merchant bank.
22. Then, the merchant bank sends a message to the system server that the transaction has successfully completed.
23. Then the system server sends the commit transaction message to the Controller Agent (CTA).
24. At last, CTA sends the confirmation message to Client Agent (CA).

4.2 Internal Design

The internal design of the agent based secured e-shopping system is illustrated using the internal structure of the system and the price safety check checks the price twice to ensure security.

4.2.1 Structure of the e-Shopping System

There are various shops in the e-Shopping system. Each of the shop has various lists of items. Here the internal structure of the e-shopping system is designed like the internal structure of a shopping mall in such a way that each floor contains one big shop which has various lists of items.

The internal structure of the e-Shopping system is shown in the following figure:

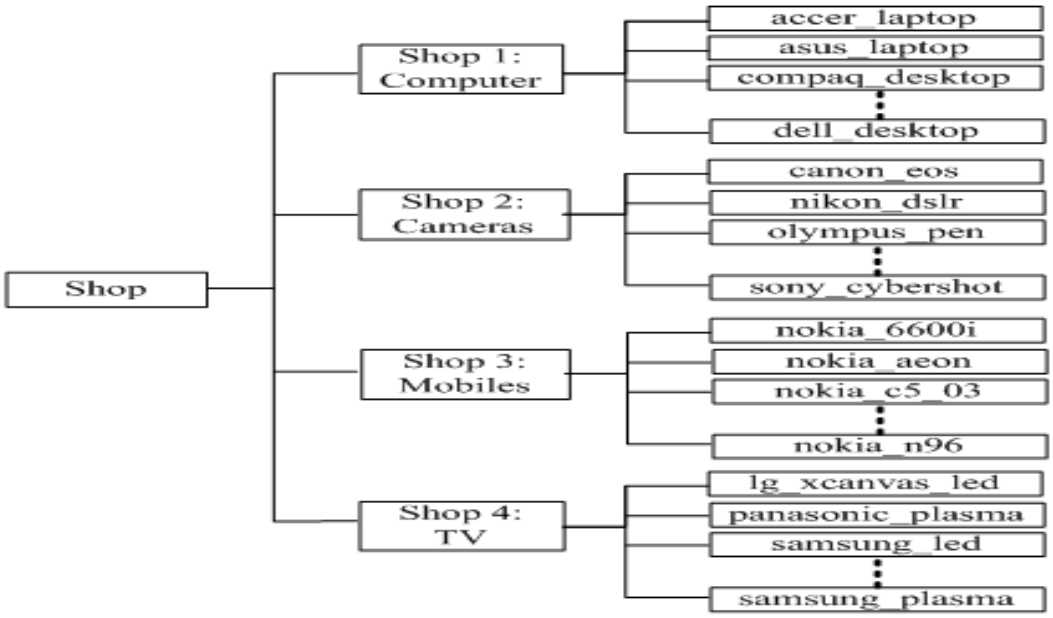

Figure 3: Internal Structure of the e-Shop

4.2.2 Price Safety Check

When the customer send the list of order item to e-shopping server, at the customer agent side total price with item list send to the server, the server will according the item list calculated the total price compare with the customer calculated the total price to check.

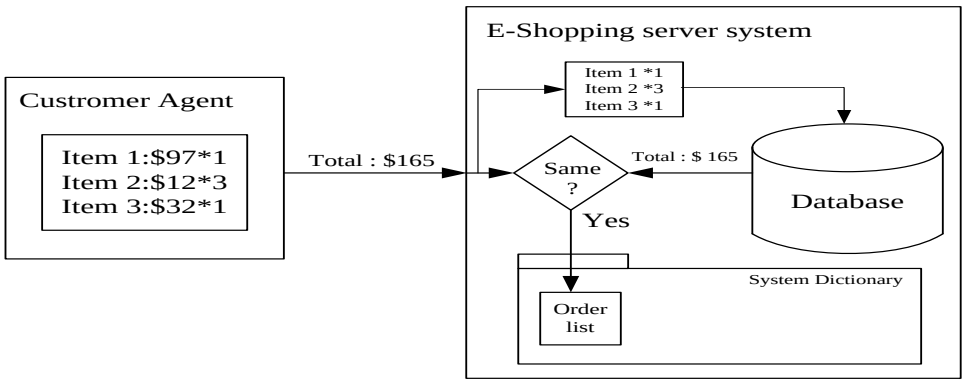

Figure 4: Price Safety Check

5. Elliptic Curve Cryptosystem [12]

The general equation for the elliptic curve is $y^2=x^3+ax+b \ mod \ p$, p is a natural prime number, and the value of a, b should satisfy the discriminate $D=4a^3+27b^2 \neq 0 \ mod \ p$ be used as the decrypting elliptic curve cryptosystem algorithm.

5.1 Pseudocode for Finding Points on an Elliptic Curve over GF (p)

```
Elliptic Curve points (p, a, b)          //p is the modulas
{
 x←0
 While(x<p)
  {
    w←(x^3+ax+b)mod p
    if(w is a perfect square in Zp)
        output(x, √w) , (x , -√w)
    x←x+1
  }
}
```

5.2 Elliptic Curve Integrated Encryption Standard (ECIES)

The best available standard for encryption and decryption is Elliptic Curve Integrated Encryption Standard (ECIES). So, the pseudo code of Elliptic Curve Integrated Encryption Standard (ECIES) is described as follows:

5.2.1 Key Generation Process

The key generation process uses the ECC algorithm to create the public and private keys for encryption and decryption, respectively. A new key pair (public key and private key) is generated when the program is executed. The outputs of this component are the public and private keys. The steps required to generate each key are as follows:

1. Bob chooses a point E (a, b) with an elliptic curve over GF (p).
2. Bob chooses a point on the curve, $e_1(x_1, y_1)$.
3. Bob chooses a random integer d.
4. Bob calculates $e_2 (x_2, y_2) = d \times e_1(x_1, y_1)$. Here the multiplication means multiple additions of points.
5. Bob announces E (a, b), $e_1(x_1, y_1)$ and $e_2(x_2, y_2)$ as his public key. He keeps d as his private key.

5.2.2 Encryption Process

The Elliptic Curve Integrated Encryption Scheme (ECIES) is used for this process. It then validates and encrypts the input message. The inputs include the public key encryption and the data items identified as user input in the system specifications. The encryption process involves the following activities:

1. Alice receives the public key from Bob.

2. Alice selects a random integer k.
3. Alice encrypts the message m to the cipher text by calculating C=($k \times e_1$, ($k \times e_2$) + m)
4. Alice sends cipher text C to Bob.

5.2.3 Decryption Process

The Elliptic Curve Integrated Encryption Scheme (ECIES) is used for this process. The input is the cipher text and the private key produced by the key generator and encryption processes, respectively. The decryption process involves the following activities:

1. Bob receives the cipher text C from Alice.
2. Bob then decrypts the cipher text by calculating:
   $m + (k \times e_2) - d \times k \times e_1 = m + (k \times d \times e_1) - (d \times k \times e_1) = m$.

5.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

Alice sends the message and the signature to the Bob. This signature can be verified only by using the public key of Alice. Since the Bob knows Alice's public key, it can verify whether the message is indeed send by Alice or not.

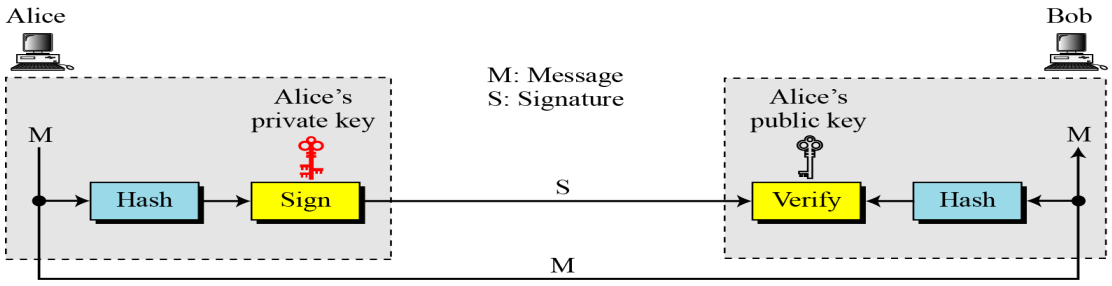

Figure 6: Signing the Digest [12]

ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups. Sender 'A' have a key pair consisting of a private key d (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key $e_2(x_2, y_2) = d \times e_1(x_1, y_1)$ (e_1 is the generator point/base point, an elliptic curve domain parameter). An overview of ECDSA process is defined below.

5.2.3 Signature Generation

For signing a message m by sender Alice, using Alice's private key d

1. Calculate e = HASH (m), where HASH is a cryptographic hash function, such as SHA-256
2. Select a random integer k from [1, n − 1]
3. Calculate $r = x_2 \pmod n$, where $(x_2, y_2) = k \times e_1$. If r = 0, go to step 2
4. Calculate $s = k^{-1}(e + d \times r) \pmod n$. If s = 0, go to step 2
5. The signature is the pair (r, s)

5.2.4 Signature Verification

For B to authenticate Alice's signature, Bob must have Alice's public key e_2

1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate $w = s^{-1} \pmod n$
4. Calculate $u_1 = e \times w \pmod n$ and $u_2 = r \times w \pmod n$
5. Calculate $(x_2, y_2) = u_1 \times e_1 + u_2 \times e_2$
6. The signature is valid if $x_2 = r \pmod n$, invalid otherwise

6. Implementation

To implement the agent based secured e-shopping system, we are using JADE (Java Agent Development Environment) 4.01 and Elliptic Curve Cryptography (ECC). JADE is a software platform that provides basic middleware-layer functionalities which are independent of the specific application and which simplify the realization of distributed applications that exploit the software agent abstraction. A significant merit of JADE is that it implements this abstraction over a well-known object-oriented language, Java, providing a simple and friendly API. The following simple design choices were influenced by the agent abstraction.

To implement the Elliptic Curve Cryptography for providing the security for e-payment in the e-shopping system, the java cryptographic package and a third party security provider (Bouncy Castle) [21] is used. In this e-shopping system, every time, the application is executed, a new key pair (private key and public key) is generated. Here, we are using ECC-192 and SHA-256withECDSA.

6.1 JADE Architecture

JADE platform is composed of agent containers that can be distributed over the network. Agents live in containers which are the Java process that provides the JADE run-time and all the services needed for hosting and executing agents. There is a special container, called the *main container*, which represents the bootstrap point of a platform: it is the first container to be launched and all other containers must join to a main container by registering with it.

The containers are identified by simply using a logical name; by default the main container is named 'Main Container' while the others are named 'Container-1', 'Container-2', etc.

When the main-container is launched, two special agents are automatically instantiated and started by JADE [11].

1. **The Agent Management System (AMS)** is the agent that supervises the entire platform. Every agent is required to register with the AMS (automatically carried out by JADE at agent start-up) in order to obtain a valid AID.
2. **The Directory Facilitator (DF)** is the agent that implements the yellow pages service, used by any agent wishing to register its services or search for other available services. The JADE DF also accepts subscriptions from agents that wish to be notified whenever a service registration or modification is made that match some specified criteria.

This GUI which is illustrated in Figure 7 is actually provided by a JADE system agent called the Remote Monitoring Agent (RMA) and allows a platform administrator to manipulate and monitor the running platform.

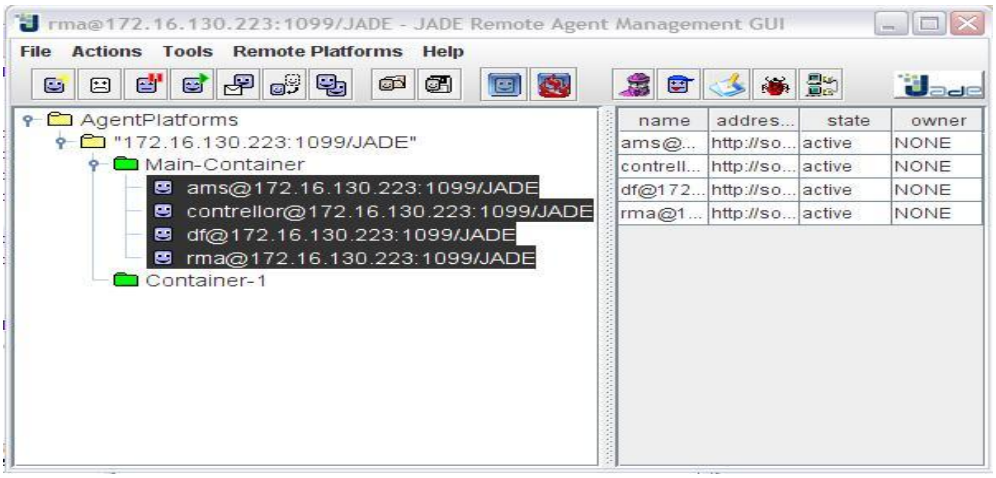

Figure 7: Jade GUI

6.2 Controller Agent (CTA)

The Controller Agent (CTA) is created by executing the program "ControllerAgent.java" and the design frame of controller is created by "ControllerAgentGui.java". The controller works as the agent manager of the e-shopping system. It creates the Client Agent (CA) as per request and it has the ability to kill the Client Agent (CA) to stop any malfunction of the system. It also sends the commodity information or the item details from the server side to the Client Agent (CA). By executing the java program "listitem.java", the CTA automatically counts the number of available items for each shop and also any number of items can be added into or deleted from the database. The Controller Agent (CTA) encrypts and signs all the confidential data and sends to the bank and produces the encrypted and signed receipt document using ECC and ECDSA respectively. The controller agent GUI is illustrated as follows:

Figure 8: Controller Agent GUI

6.3 Client Agent (CA)

In the Figure 8 if we click the button "Login agent" then a new Client Agent will be created. After that, customer provides the password. If it is correct, then the customer enters into the e-shopping system with the help of Client Agent (CA). The design frame of the Client Agent GUI is build by executing the java program "ClientAgentGui.java". The CA sends the credit card information to the CTA and CTA checks verifies and updates the agent information to the database. Besides these, CA shows the customer the various shops in the e-shopping system and the total amount which is received from the CTA.

When the customer click the button, "Buy the all" in figure 9, the credit card number and the password is encrypted with the ECC public key to provide the confidentiality and integrity and this information is sent to the bank for secure transaction. Bank decrypts this information using ECC private key and makes the transaction successful.

In this way the Client Agent works on behalf of the customer. This is illustrated in the Figure 9, 10, 11 and 12 respectively:

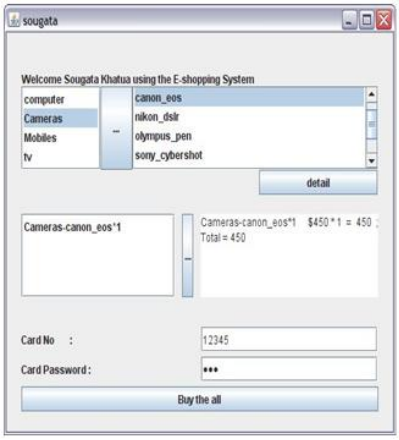

Figure 9: Client Agent GUI

Figure 10: Item Details

Figure 11: Transaction details

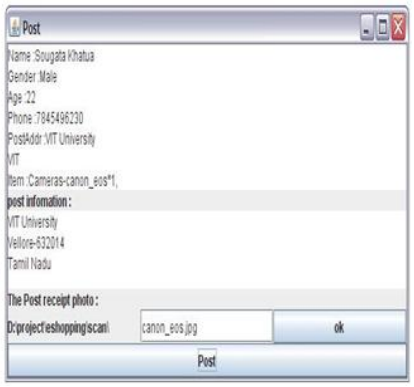

Figure 12: Billing details

When the customer gets the bill as illustrated in Figure 11 and gets the message and "Receipt No." as illustrated in Figure 12, the transaction successfully completed. The message as illustrated in Figure 12 is treated as the confirmation message. The customer keeps the "Receipt No." and later it verifies this number when the shopping items are to be

delivered to the corresponding address.

The e-shop manager can see the "Receipt No" and the corresponding order details of the customer and using this information, the manager post the corresponding order to respective address to maintain the integrity of the delivery of the product which is shown in Figure 13, 14 and 15.

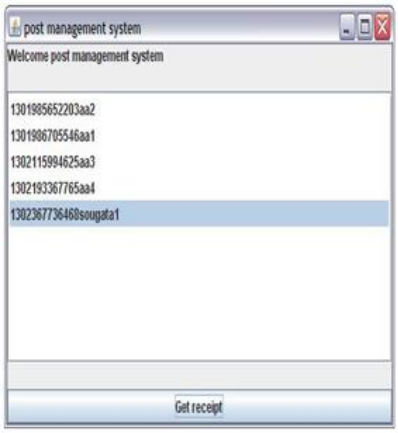

Figure 13: Post Management System **Figure 14: Post Details**

When we click the button "Post" in Figure 14, the details which is selected Figure 13 in post management system of the corresponding receipt number will be deleted and the new receipt will be generated and the information in the receipt document is encrypted with ECC. The post manager decrypts the information and sends the receipt bill which is shown in figure 15 and it is delivered to the customer.

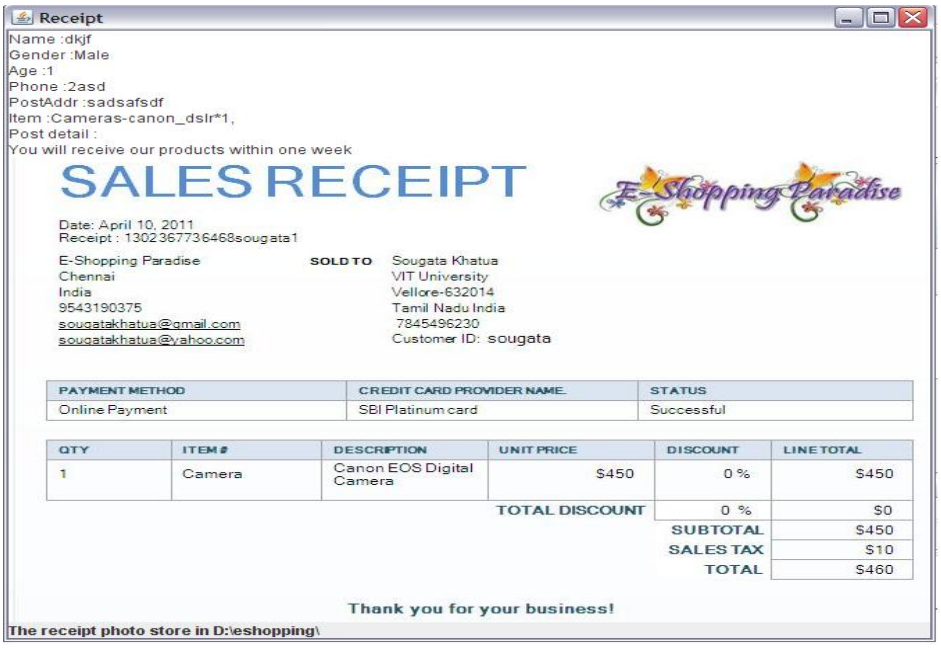

Figure 15: Sales Receipt

6.4 Message Passing between the Agents

From proposed system design viewpoint, Figure 16 represents message sequence for the connection between the GUI agent and Client Agent, Controller Agent, RMA, AMS, DF using a series of requests through JADE agent ACL Messages.

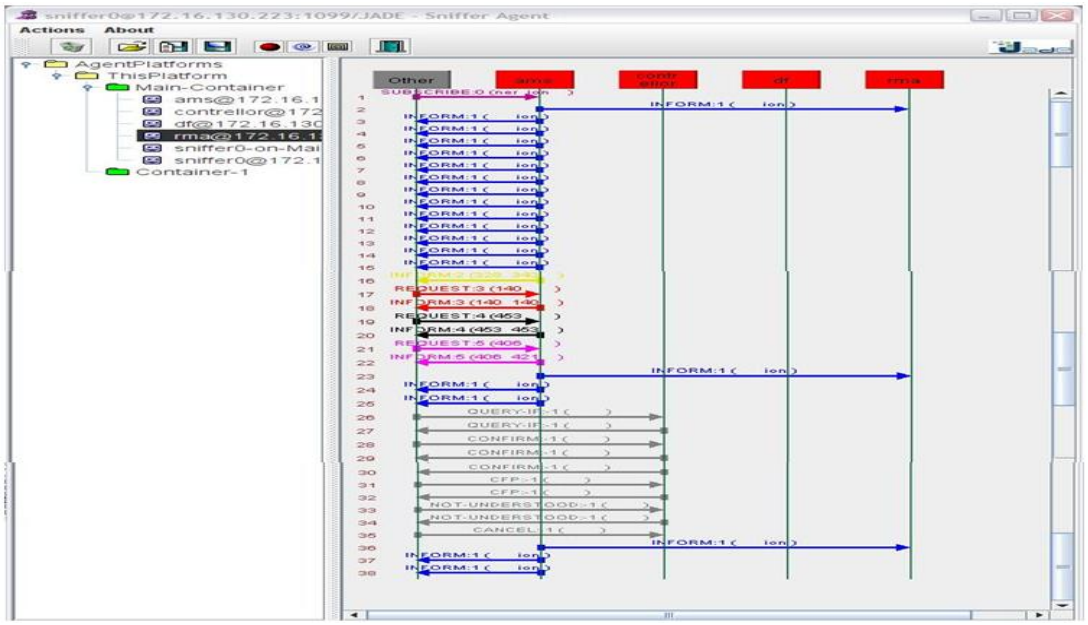

Figure 16: Message Passing between the Agents

7. Evaluation

After completion of the system's implementation phase, multiple tests were conducted by generating multiple keys and multiple signatures to ensure that each process and the entire system were operating properly.

So, here the ECIES testing and ECDSA testing is done to check the algorithm works properly and the system is running properly or not.

The results generated by the ECIES test are displayed on Table 5.

Table 5: Process State of ECIES

Test No.	*Public Key*	*Private Key*	*I = Input O = Output C = Ciphertext*	
1.	X: 8c53b724e53b27a8b25ad122e4a34d98d08e814badd94d7a Y: 57e2d8d57e8bc73fbab824bd08e70848cd9cd67c7d21ee7e	fd0c25b1	***I***	Sougata Khatua
			C	+L/nmjYchTqCl25RomRjFWIzf/xiiIE UsLnW6x7Q
			O	Sougata Khatua
2.	X: ecb0f0aa45469965b201e03dcf227b05a217aa8c4c4825f9 Y: 9bbcf5dd5bf2b23bd9503940242fc76eb5bcf82b0336f124	35c30e2	***I***	1234123412341234
			C	fDaZnSOI2Qg2nWg8NuU4KqE+pyug WgpRRSffXRyfCS/FxA==
			O	1234123412341234

The results generated by the ECDSA test are displayed in Table 6.

Table 6: Process State of ECDSA

Value Constraints	*Value*	*Signature*	*Signature Verification*
Delivery Address Line 1	VIT University	MDYCGQDaaGM3rmkP+jKZnioVBzoTTA4Oh5aXLK 8CGQCQv7OE6MP4botQPJiurEW6DF0QtRN4LK8=	True
Delivery Address Line 2	Vellore -14	MDQCGCsER8N6bK1jyA1Z4+GDyP6+5vSeROP68wI YZDuge52HySwl4/AC++yhvjL1dcsVGUOW	True
Delivery Address Line 3	Tamil Nadu	MDQCGAjhkVKLJvQRX5UB0q62bxKSxIoid9AmYAI YKcEiHWbKLR8uJ9ug8iiugGDF8BP7b2RX	True
Total Amount	16,200	a+kQv6fjF5UfbYv4eUKCz6U3iOtxOxm9yyNt5HqtovH HcVi6C4Ym7NHiglpt/NcRuitjor5BMT4W dV0o4epjpHzEybU4Pf1l8ZO3	True

Table 5 illustrates that the system performs the encryption and decryption properly and check for any fault is there or not to encrypt and decrypt the confidential data. Table 6 shows the system performs signature generation and signature verification properly to achieve the integrity, authentication and non repudiation.

8. Performance Analysis

After the completion of the development phase, the performance of the agent based secured e-shopping system using ECC is analyzed against the secured e-shopping system using ECC without agent technology.

The Table 7 summarizes the security strength and the key length of the ECC, RSA, Elgamal and DSA. From the table 7 it is clear that ECC needs much less key size to achieve the required level security. That's why ECC is used to provide the security of the e-Shopping system. As the validity of ECC-160 is up to 2010, and now it is 2011, ECC-192 and SHA-256withECDSA are used in this project to provide security to the e-shopping system.

Table 7: Summarization of Public Key System [20]

ECC	*RSA/DSA /Elgamal*	*MIPS years to attack*	*Key size ratio*	*Protection Lifetime*
160	1024	10^{12}	1:6.4	Up to 2010
224	2048	10^{24}	1:9.14	Up to 2030
256	3072	10^{28}	1:12	Beyond 2031
384	7680	10^{47}	1:20	
512	15360	10^{66}	1:30	

Graph Comparison of key size:

From this graph, it is clear that ECC needs much less key size compared to RSA and DSA to achieve the required level of security.

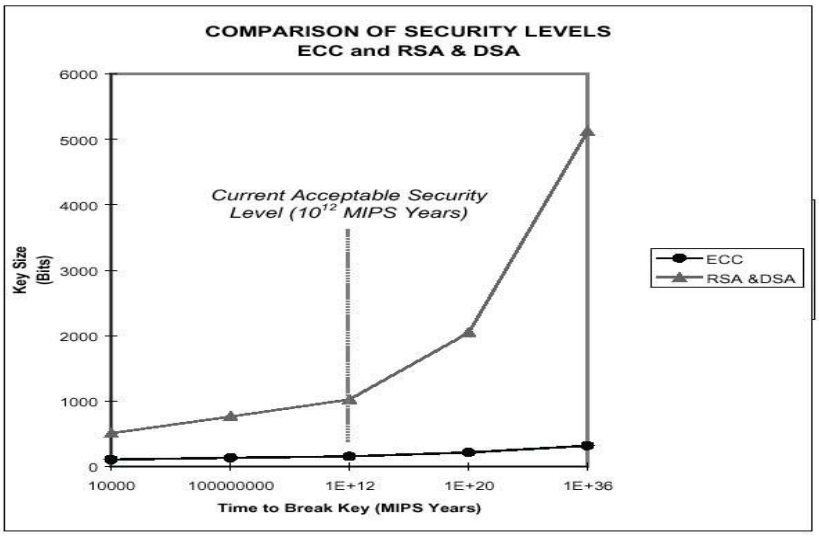

Figure 17: Comparison between ECC and RSA/DSA [19]

8.1 Analysis of Execution Time

Here, the analysis of the agent based secured e-shopping system is done with the secured e-shopping system which do not use the agent technology.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with 3GB RAM, Windows XP using JAVA

The comparison table and graph to analysis the performance in terms of execution time is given below:

Table 8: Performance Analysis of Execution Time

	Without Agent secured e-shopping system			*Agent based secured e-shopping system*		
Key size	ECC-160	ECC-192	ECC-224	ECC-160	ECC-192	ECC-224
Execution time	110 sec	122 sec	133 sec	76 sec	88 sec	101 sec

Graph comparison of execution time:

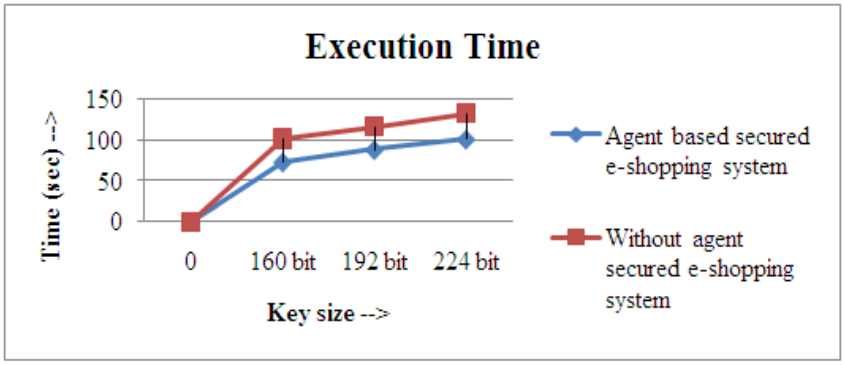

Figure 18: Execution Time

From the above figure, Figure 18 and Table 8, it is clear that agent based secured e-shopping system using ECC needs much less time about 35% less time than the without agent secured e-shopping system using ECC.

8.2 Analysis of CPU Utilization

Here, the analysis of the agent based secured e-shopping system is done with the secured e-shopping system which do not use the agent technology.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with 3GB RAM, Windows XP using JAVA

The comparison table and graph to analysis the performance in terms of CPU utilization is given below:

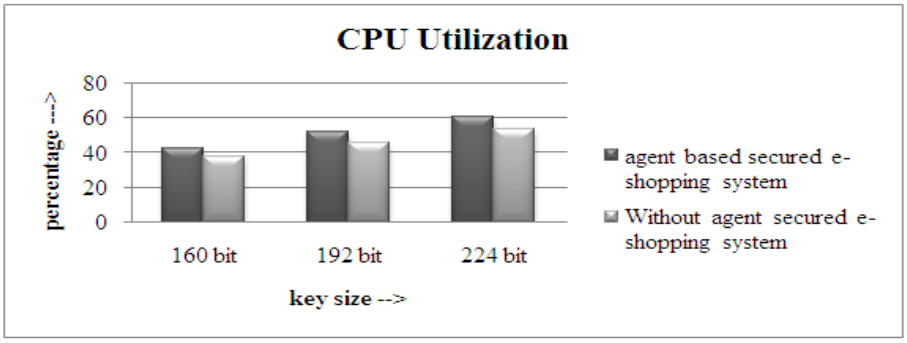

Figure 19: CPU Utilization

From, the above figure, it is clear that, the agent based secured e-shopping system uses little bit more resource i.e. CPU utilization than the general without agent secured e-shopping system.

Hence, from the above, it is clear that the agent based e-shopping system performs better than the general web based e-shopping system. Agent based secured e-shopping system saves enormous time taken by the general without agent secured e-shopping system with the cost of little bit more using the resources.

9. Conclusion and Future Work

The rapid development of the Internet and e-commerce including online shopping made it important that the need to automate shopping process on Internet and provide more personalized information services for customers. The above analysis suggests that the agent based e-shopping system performs better than the e-shopping system which is not based on the agent technology.

In future, an intelligent shopping system can be developed. In this work, a multi-agent system to provide shopping service for the commodities that a consumer does not buy frequently. The system integrates built-in expert knowledge [17] and the customer's current needs, and recommends optimal products based on multi-attribute decision making method [16].

In future the security of the e-shopping system can be provided using *Hyper Elliptic Curve Cryptography (HECC).* This algorithm needs only 80 bit long key to achieve the required level security. So it needs less key size than ECC.

References

[1] Ritu Gupta[1], Gaurav Kansal[2], "A Survey on Comparative Study of Mobile Agent Platforms", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No.: 3, Page: 1943, **(2011)** March

[2] Vikas Rattan, "E-Commerce Security using PKI approach", International Journal on Computer Science and Engineering (IJCSE), **(2010)** Vol. 02, No. 05, 1439-1444

[3] Dr. S.S.Riaz Ahamed, "The Influence of scope and Integrated Experimental Approach to safe Electronic Commerce", International Journal of Engineering Science and Technology, **(2010)** Vol. 2(3), 448-456

[4] Rupesh Kumar, Mario Muñoz Organero, "XML Secure Documents for a Secure e-Commerce Architecture", Global Journal of Enterprise Information System,Volume-2 Issue-1, **(2010)** June

[5] Ziming Zeng, "An Agent-based Online Shopping System in E-commerce", Computer and Information Science, Vol.2, No. 4, **(2009)** November

[6] Richard Ssekibuule and Jose Ghislain Quenum, "Security Analysis of an Agent-Mediated Book Trading Application", International Journal of Computing and ICT Research, Special Issue Vol. 3, No. 1, **(2009)** October

[7] Michał Drozdowicz,Maria Ganzha, Maciej Gawinecki, Paweł Kobzdej, Marcin Paprzycki, "DESIGNING AND IMPLEMENTING DATA MART FOR AN AGENT-BASED E-COMMERCE SYSTEM", IADIS International Journal,Vol. 6, No. 1, pp. 37-49,ISSN: 1645 – 7641,2008

[8] I. K. Salah, A. Darwish, and S. Oqeili, "Mathematical attacks on RSA cryptosystem," Journal of Computer Science, pp. 656-671, **(2006)** August

[9] Braz, Christina,Ncho, Ambroise, "MBAOS: A Mobile Bargain Agent for Online Shopping", IFT6862 ARTIFICIAL INTELLIGENCE **(2003)** Winter

[10] Kwang Hyoun JOO, Tessuo KINOSHITA,Nario SHIRATORI, "Design and Implementation of an Agent Based Grocery Shopping System", IEICE, Vol.E83-D,NO.11, **(2000)** November

[11] Developing Multi-Agent Systems with JADE Fabio Bellifemine, Giovanni Caire, Dominic Greenwood, Page No.: 30-50, Copyright © 2007 John Wiley & Sons, Ltd **(2007)**

[12] Behrouz A. Forouzan, Debdeep Mukhopadhyay, " Cryptography and Network Security", Tata McGraw-Hill , Page No.:358 © 2010 by McGra-Hill Companies **(2010)**

[13] Courtney McTavish,Suresh Sankaranarayanan, "Intelligent Agent based Hotel Search & Booking System", Proceedings of the 9th WSEAS International Conference on TELECOMMUNICATIONS and INFORMATICS, **(2009)**

[14] Hesham M. Kamel,Moza Al-Nasseri,Maryam Al-Aryany, Hamda Al-Awar, "The Smart Shopping System (SSS): An Adaptive Eshopping Application for Reflecting the User's Personal Model", ftp://amd64gcc.dyndns.org/WORLDCOMP06/EEE4609.pdf

[15] Tan Xueqing, Zeng Ziming "A Shopping Model in Agent-mediated Electronic Commerce", http://www.seiofbluemountain.com/upload/product/200911/2006zxqyhy09a1.pdf

[16] Javier Bajo, Ana de Luis, Angelica Gonzalez, Alberto Saavedra and Juan M.Corchado, "A Shopping Mall Multiagent System: Ambient Intelligence in Practice" http://bisite.usal.es/webisite/archivos/publicaciones/otrosCongresos/2006/wucami06-shoppingmallambientintelligencev2.pdf

[17] Zeng Zi-ming and Meng Bo," An Intelligent Shopping System Based on Multi-agent Collaborative Working Model", CCECE/CCGEI, Saskatoon, May 2005,0-7803-8886-0/05, © 2005 IEEE **(2005)**

[18] Marchany, R. and Tront, J. " E-commerce Security Issues", hicss, p-193, 35th Annual Hawaii International Conference on System Sciences(HICSS'02):2002-Volume 7, IEEE **(2000)**

[19] Vipul Gupta, Douglas Stebila[*], Stephen Fung[*], Sheueling Chang Shantz, Nils Gura, Hans Eberle, "Speeding up Secure Web Transaction using Elliptic Curve Cryptography", Sun Microsystems, http://research.sun.com/projects/crypto

[20] http://www.trustis.com/pki/fpsia/guide/the-abc%27s-of-secure-electronic-commerce.pdf, White paper, **(2001)**

[21] http://www.bouncycastle.org

Authors

Sougata Khatua has received his B.Sc (Computer Science) degree from Midnapore College under Vidyasagar University**,** Paschim Medinipur, West Bengal, India and he has done his M.Sc (Computer Science) from VIT University, Vellore, Tamil Nadu, India. Currently he is an employee of Cognizant Technology Solutions. His areas of interest are Artificial Intelligence, Intelligent Distributed Computing, Cryptography and Information Security.

Arijit Das has received his B.Sc (Computer Science) degree from Midnapore College under Vidyasagar University**,** Paschim Medinipur, West Bengal, India and he has done his M.Sc (Computer Science) from VIT University, Vellore, Tamil Nadu, India. Currently he is an employee of Cognizant Technology Solutions. His areas of interest are Intelligent Distributed Computing, Cryptography and Information Security.

Zhang Yuheng received B.Sc (Computer Science) degree from Central South University of Forestry and Technology, Changsha, Hunan Province, China and also Vellore Institute of Technology University, T.N, India in 2009 under 3+1 top up program. Currently he is a final year post graduate student of M.Sc (Computer Science) at VIT University, Vellore, T.N., India. His areas of interest are Intelligent Distributed Computing and cryptography.

Dr. LI Li is an Associate Professor at the International School of Software at Wuhan University, Wuhan, China. Her research interests include Data Privacy and Network Security, Security Protocol Analysis and Embedded System.

Dr.N.Ch.S.N. Iyengar (M.Sc,M.E,Ph.D) is a Senior Professor at the School of Computing Science and Engineering at VIT University, Vellore, Tamil Nadu, India. His research interests include Agent based Distributed Computing, Data Privacy and Security, Cryptography, Intelligent computational methods and Bio informatics. He has authored several textbooks and had nearly 100 research Publications in International Journals. He chaired many international conferences and delivered invited/ technical lectures/ keynote addresses besides being International program committee member.