Agent Based Secured Online Hotel Booking System

Jaya Subalakshmi R.[1], N.Ch.S.N. Iyengar[2], Sougata Khatua[3], Haleema[4]

[1,2,3,4]School of Computing Science & Engineering, VIT University
Vellore-632014, Tamilnadu, India.

Abstract

The ever-increasing growth of Internet users created a new business paradigm and opened up a new revenue model for the businesses which is termed as e-business or e-services. One such service is e-hotel booking service. Before the deployment of e-services, the process of finding an appropriate hotel in a required place was a time consuming and a tedious job and was done mostly through human agents who may not be trust-worthy. So people find it convenient and easy to book hotels over the Internet via the e-hotel booking services. Use of mobile agent technology for the development of online hotel booking system has addressed performance, automation and flexibility requirements of distributed applications. As e-transactions have increased tremendously in the past few years and Internet being a heterogeneous and non secure environment, it gives rise to many security issues such as privacy, authenticity, integrity, and non-repudiation that are to be addressed by systems in which face to face interaction is not possible. Most of the online hotel booking systems does not provide the required level of security service because of which many problems arise in the systems such as denying, losing, misusing, stealing, double-spending etc. This paper addresses all the above security issues by developing a agent based Secured Online Hotel Booking System using the combination of Elliptic Curve Cryptography, AES and SHA-256.

***Keywords*:** *JADE, Symmetric Key Cryptography, Asymmetric Key Cryptography, Hash function, Hotel booking*

1. Introduction

The development of Internet and Web 2.0 technologies with their immeasurable benefits forces the businesses to adapt to e-services. As the Internet being a distributed heterogeneous environment and the applications that are built on top of distributed systems demand flexible and intelligent solutions, agent-based technologies have been developed with the aim of providing solutions for the emergent problems and for managing the complexity that arise in this arena. Agent-based systems have become one of the most vibrant and important areas of research and development in the recent years. *Agents* can be defined to be autonomous, problem-solving, computational entities capable of effective operation in dynamic and open environments. Agents are often deployed in environments where they can interact and may cooperate with other agents on a user's behalf that have possibly conflicting aims. Such environments are known as *multi-agent systems*.

The online hotel booking system delivers a variety of services that are useful for the people who travel frequently to various places all over the world. Use of mobile agent technology for the development of online hotel booking system has addressed performance, automation and flexibility requirements of distributed applications. Security for customer's banking details in electronic transactions is an important concern while using such services.

The major security requirements for an online hotel booking system are identified to be the following:

Confidentiality: Customer's banking details must be kept confidential when he/she makes an online payment against a hotel booking. Confidentiality for customer's banking information is ensured by encrypting them before actually disseminating those data.

Integrity: e-transaction details such as transaction amount, beneficiary name and account number must not be altered (Integrity of transaction). The transaction receipt indicating the booking confirmation must be delivered to the customer without any alteration (Integrity of receipt delivery).

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

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

Availability: It ensures that end system (host) and the service are available for access all the time to the authorized user.

Accountability: The identities of all users are assured and the users are made responsible for their action [1].

Copy protection: This feature ensures protection from unauthorized copying of intellectual information [2].

The security features for the proposed online hotel booking system is provided based on the following components of cryptography:

Public Key Cryptosystem (PKC) can be used 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)* [3] are based on PKC.

Digital signature: This is used to ensure integrity of information, authenticity of the user and availability of the information to the authenticated user.

Password based authentication: It is used to verify the users' identity. It is the simplest and oldest method of entity authentication.

The rest of the paper is organized as follows: Chapter 2 describes the related work in this area, identifies the research gap and the need for this proposal. Chapter 3 provides a description on the various technologies used in developing the proposed system. Chapter 4 describes the functionalities of software agents deployed in the proposed

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

system, depicts the architecture diagram and also explains the sequence diagrams depicting the order of activities in processing the user query messages and transaction related messages. Chapter 5 describes the experimental set up and the implementation procedures. An evaluation of the proposed system under various parameters is carried out in chapters 6 and 7. Chapter 8 concludes the paper and also identifies the direction towards future work.

2. Related Work

The information technology rebellion plays a crucial role in Internet. The progress in web technologies promotes the progress of electronic services. E-services have a tremendous growth in the recent years due to the advancements in Internet technologies. Rust and Kannan [4] views an e-service as an interactive, Internet-based customer services and content-centered, determined by the customer and incorporated with associated organizational customer support practices and technologies with the goal of spiraling the service provider and customer relationship. Moreover in Internet, the real power of computers is realized through distributed, open, dynamic and heterogeneous systems which can interact, span organizational boundaries, and operate effectively within rapidly changing circumstances [5]. In the context of addressing such requirements, agent technologies have been developed with the aim of providing solutions for the emergent problems and for managing the complexity that arise in this arena.

Software agents are used to implement highly modular e-services that are inter-operable, flexible, co-operative and autonomous. The desire for more cost efficiency and less sub-optimal business processes drives the employment of agent technology in e-Business. Bellifemine [6] state that the basic intelligent property of agents lies in the autonomy of operation, coordination and negotiation between agents for communication that leads to efficient problem solving. Such emerging agent technology has been applied in almost many fields like shopping, healthcare, online hotel booking etc. Sivakumar[7] incorporated agent technology to enhance the effectiveness of e-learning strategies by proposing a dynamic generation of contents and expert query management system. He describes in his paper the combination of computational intelligence of E-learning system and properties of intelligent agents. Srinivasan[8] presented a conceptual framework for decision support systems based on Multi-agent System using Data Mining and case-based reasoning for automation of work flow based systems. Pooja Jain[9] proposed an agent-based knowledge service-oriented system framework to reflect the distributed, flexible and hierarchical characteristics of an enterprise system. The basic aim of the multi-agent knowledge management system is to increase the throughput and to reduce the response time. Tavish [10] proposed an agent based hotel booking system, where the agent involves in the activities of searching and booking of hotels from the mobile devices using JADE LEAP technology. Qi Wei[11] in their research proposed a framework to recognize the factors that influence consumers choice of channels in the online hotel booking, where the results specifies that both the opinion of channel and socio-demographics are important factors. Kuang [12] developed an Online Hotel Booking Consumer Satisfaction model in which the final results show that easy exploitation of website makes the customer satisfaction more significant, pursued by responsiveness and reliability of the website.

However Security is the major concern in any network. Shazia Yasin[13] states the key dimensions of E-commerce security to be Access Control, Privacy/Confidentiality, Authentication, Non Repudiation, Integrity and Availability. Vineeta Khemchandani [14] presented a software-based approach, which combines digital signature technology with robust watermarking technique to achieve authenticity, confidentiality, integrity and restricting alteration and forgery in information. Ackerman [15] in his paper discussed about different security techniques like Public Key Infrastructure (PKI), Digital Signature, and Symmetric Key Systems etc. The online hotel booking system [10] is based on popular Secure Socket Layer (SSL). But currently there exists more efficient and strong security algorithms compared to the algorithms which are used in SSL. Lawrence [16] discussed about the biometric security system like finger print or retina test in his work. As biometric devices are expensive, it is not considered to be a feasible security solution.

From the literature survey carried out as stated above, it has been identified that there is a great need for well defined security solutions in the development of online hotel booking systems. Here in this paper, a proposal for agent based security solutions using a hybrid protocol is made which ensures strong security at various levels of hotel booking process.

3. Technologies used in Proposed System

The methodologies used for developing agent based Secured Online Hotel Booking System (SOHBS) are described below:

3.1 Web based mobile agent

Java Agent Development Environment (JADE) framework is used with Java Server Pages (JSP) to address the various issues that arise in delivering e-services in general and also to increase the performance, flexibility and automation of the proposed system in particular.

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 Java features which is an Object Oriented Programming language and also third-party libraries on offer, and thus offers a rich set of programming abstractions allowing

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

developers to construct JADE multi-agent systems with relatively minimal expertise in agent theory.

JADE platform is composed of agent containers that can be distributed over the network. Agents live in containers which are Java processes that provide 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 the 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 [6].

1. *The Agent Management System (AMS)* is the agent that supervises the entire platform. Every agent is required to register with the AMS 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 GUI provided by a JADE system agent called the Remote Monitoring Agent (RMA) is shown in figure 4 which allows a platform administrator to manipulate and monitor the running platform.

Using the JADE agent technology, the proposed agent based Secured Online Hotel Booking System (SOHBS) has the following characteristics [6]:

- *Autonomy:* The system has the autonomous transaction facility. It reduces the user intervention during booking activity.
- *Agent Collaboration and Cooperation:* Agents collaborate and cooperate with each other in order to respond to users' requests.
- *Security:* The system ensures security at various levels of the hotel booking process.
- *Scalability:* Using JADE technology, the system can easily scale up to 1500 agents and 300000 ACL messages.
- *Faster:* The proposed e-hotel booking system is faster than the existing systems.

3.2 Hybrid Security Model

Like any distributed system is subject to security threats such as eavesdropping, corruption, masquerading, denial of service, replaying, and repudiation, a mobile agent system is also subject to similar set of threats [17]. Therefore, issues such as encryption, authorization, authentication, and non-repudiation should be addressed in a mobile agent system. Moreover, a secure mobile agent system must protect the hosts as well as the agents from being tampered by malicious parties. To overcome these types of security issues, a hybrid security model is proposed which uses combination of Public Key Cryptography and Private Key Cryptography to take the advantages of both. In addition to these, hash function is used to provide integrity of the message.

Private Key Cryptography: AES is selected as private key cryptography to provide confidentiality for secret messages because till now there is no major attack reported against AES. Here AES-192 is used to provide security for confidential information.

Public Key Cryptography: Elliptic Curve Cryptography is the public key cryptosystem and it is used to ensure authentication, integrity and non-repudiation service.

Hash Function: SHA-256 is used as a hash function in combination with Elliptic Curve Digital Signature (ECDSA) to ensure integrity of the messages. Here SHA-256 is chosen because there is no major attack reported against SHA-256 hash function. As integrity is one of the most important security concerns, SHA-256 is used with ECDSA to enhance the security of the system.

4. Proposed System Design

Architectural diagram describes the overall design of the system along with their various functional components and their functionality. *Sequence flow diagram* shows how the components of SOHBS communicate with each other by exchanging messages at various points in time.

4.1 Architecture of SOHBS

The figure 1 shows the architecture of SOHBS.

4.1.1 Components of SOHBS and their Functionalities

User Agent (UA): The User Agent (UA) reads the user's preference. If the user's preference is to get the information about availability of hotels at a particular location, then UA transfers the user's request to Central Database Agent (CDA). If the user's preference is to make a hotel room booking, then UA transfers the user's request to Booking Agent (BA). UA also receives the responses of CDA and BA and displays it to the user.

Central Database Agent (CDA): The Central Database Agent (CDA) receives the user's query from the User Agent (UA) and searches the Central Database (CDB) according to the users query and passes the information fetched from CDB to UA for further processing. The most important task of this agent is to update the central database with the latest information about the hotels available all over the world. The overall functionalities of CDA include enhancing new hotel registration process, updating existing hotel information, searching the hotels according to the users' query, and deleting invalid hotel information from CDB. It maintains information such as Hotel Name, Hotel Category, Hotel Rooms Availability Status and Hotel Rooms Tariffs in the Central Database.

Booking Agent (BA): The Booking Agent (BA) receives the user's request for hotel booking or cancellation of

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

already made booking from UA. BA passes the user's booking request to the Security Agent (SA) to provide security for the user's banking details during the hotel booking process. Later it receives the money transaction details from the Security Agent (SA) once the booking process is over. This agent behaves like an intermediary between UA and SA, and it is used to improve the overall performance of the system.

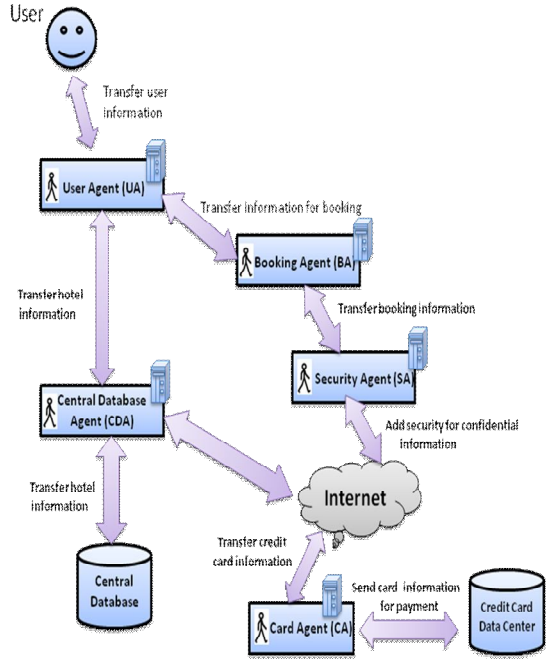

Fig 1. Architecture of SOHBS

Security Agent (SA): It is the most important agent among all the five agents deployed in SOHBS. The main responsibility of this agent is to provide security for confidential information before disseminating them over the Internet. It receives the booking related information from the Booking Agent (BA) and encrypts the confidential information such as credit card number, total amount etc. SA makes use of the hybrid protocol which uses the combination of Private and Public Key Cryptography and Hash function to provide security at various level of hotel booking process. For ensuring confidentiality, information is encrypted using AES which is a Private Key Cryptosystem. For authentication, Elliptic Curve Digital Signature (ECDSA) is used and for integrity, a combination of SHA-256 and ECDSA is used. After completion of the hotel booking process, it transfers the transaction details to the Booking Agent (BA).

Card Agent (CA): The Card Agent (CA) receives the encrypted card details and signature details over the Internet sent by the Security Agent (SA). After that it decrypts the information using AES and verifies its authenticity using ECDSA. After successful verification of the information, it sends the payment related information to the Credit Card Data Center where the money is deducted and the related information is sent back to the Card Agent (CA). The Card Agent (CA) generates a receipt for the successful payment and encrypts it using AES and generates a signature using ECDSA. It then sends the encrypted receipt and the signature to the Security Agent (SA).

The *Credit Card Data Centre* of the corresponding merchant stores information including Merchant Name, Owner Name, Credit Card Number, Credit Card Type and Maximum Credit.

4.2 Sequence Diagram

The message flows are categorized into two: User Query Messages and e-transaction related Messages.

4.2.1 User Query Messages

The sequence of activities in processing the user query message is shown in figure 2 and is discussed below:

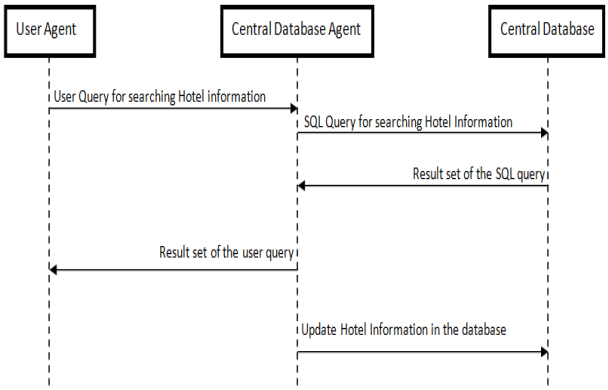

Fig 2. Sequence diagram of user query message

1. The users specify their hotel requirement details which are then converted as a user query by the User Agent (UA) and it is transferred to CDA for further processing.
2. After receiving the user query from the User Agent (UA), CDA converts it into a SQL query and optimizes the SQL query for better performance.
3. The Central Database which stores all the hotel related information is searched for the required information using the SQL query by the Central Database Agent (CDA). The result of the SQL query is then returned to the User Agent for further processing.
4. The User Agent (UA) converts the result of the user's query into a suitable format and sends it to the user console for display.

The Central Database Agent (CDA) periodically updates the central database to reflect information about various hotels available all over the world.

4.2.2 E-Transaction related Messages

The sequence of activities in processing the e-transaction messages is shown in figure 3 and is described below:

1. UA transmits the user's hotel booking request to the Booking Agent (BA).

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

2. BA collects the booking related information and sends it to the Security Agent (SA) for providing security at various levels of the e-transaction process.

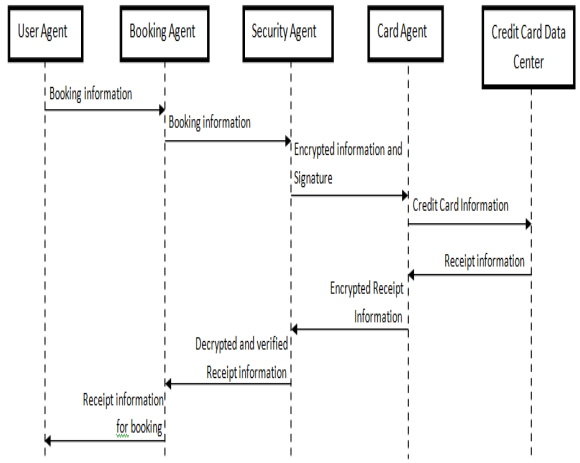

Fig 3. Sequence diagram of e-transaction related messages

3. The Security Agent (SA) encrypts the confidential information such as credit card number, card expiry date, etc using AES, applies SHA-256 on the message to create message digest in order to ensure the integrity of the message and uses Elliptic Curve Digital Signature (ECDSA) on top of message digest to create a digital signature to ensure the authenticity of the user. The secured message is then sent to the Card Agent (CA) over Internet for further processing.
4. The Card Agent (CA) receives the card details from SA, decrypts the confidential information, verifies the integrity of the data and also checks the authenticity of the card holder using the same set of algorithms used by the Security Agent (SA).
5. After successful verification of information, the Card Agent (CA) sends the Credit Card related information to the Credit Card Data Center.
6. After deducting the money from user account, it sends the receipt information to the Card Agent (CA).
7. The Card Agent (CA) encrypts the information and generates the signature using Elliptic Curve Digital Signature (ECDSA) with the combination of SHA-256. After that it sends the cipher text and the signature to the Security Agent (SA).
8. The Security Agent (SA) decrypts the cipher text and verifies the signature using the same set of algorithms used by the Card Agent (CA).
9. SA sends the receipt information to BA.
10. BA generates a receipt and sends it to UA.
11. UA displays the booking receipt onto the user console.

5. Implementation

To implement the agent based Secured Online Hotel Booking System, JADE (Java Agent Development Environment) 4.01, AES-192, ECDSA-192 and SHA-256 is used. Java cryptographic package and a third party security provider (Bouncy Castle) [18] is used to implement hybrid security protocol.

5.1 Implementation of User Agent

The algorithm for generation of User Agent (UA) and implementation of User Agent functionalities are shown in table 1.

Table.1. Algorithm for implementation of User Agent Functionalities

Algorithm	Generation of User Agent & Implementation of User Agent Functionalities.
Input	Agent Name(User_Agent), Agent Class that describes the agent behavior
Output	AID of User_Agent and the User Query for hotel information request and hotel booking request.

Procedure	Begin
	1. Create a JADE class that inherits jade.core.Agent class
	2. Override Setup() method
	3. Display AID of the created agent.
	4. Add an agent behavior(simple behavior)
	a. ReadUserRequest()
	b. CreateQuery()
	c. If (request = “HotelRegistrationRequest”)
	SendUserQueryToCDA();
	ReceiveResponseFromCDA();
	If(request = “HotelInformationRequest”)
	SendUserQueryToCDA();
	ReceiveResponseFromCDA();
	Else if(request = “HotelBookingRequest”)
	SendUserQueryToBA();
	ReceiveResponseFromBA();
	Else if(request=”BookingCancelRequest”)
	SendRequestToBA();
	ReceiveresponseFromBA();
	d. ConvertQueryResponse();
	e. DisplayResponseToUser();
	End

The snapshots in the figures 4 and 5 show the JADE GUI and the functionalities of User Agent.

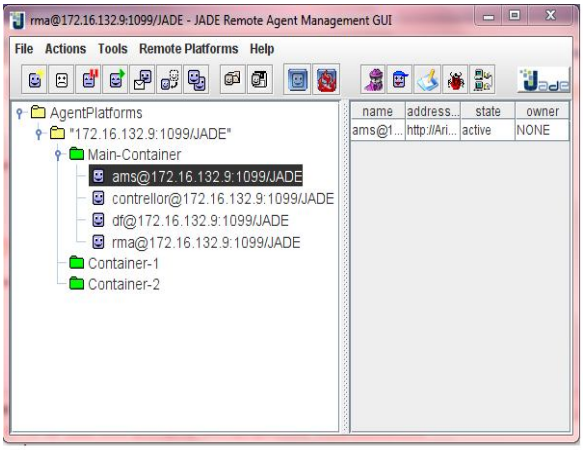

Fig 4. JADE GUI

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

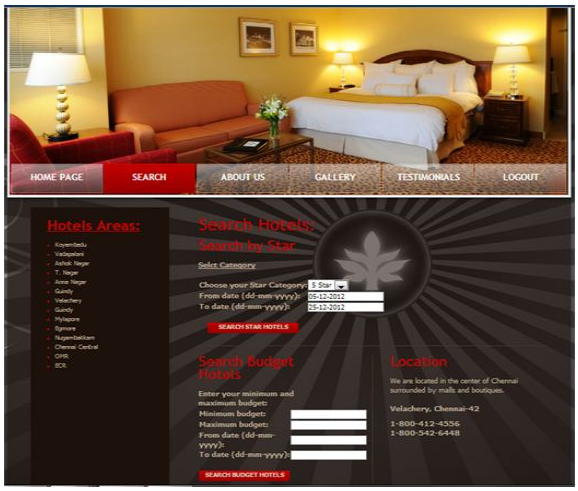

Fig 5. Hotel search details

5.2 Implementation of Security Agent

The algorithm for implementation of Security Agent (SA) functionalities is shown in table 2.

Table. 2. Algorithm for Implementation of Security Agent Functionalities.

Algorithm	Implementation of Security Agent Functionalities.
Input	Users' Credit/ Debit Card Details to make online hotel booking.
Output	Encrypted message to ensure confidentiality, message digest to ensure message integrity, digital signature to ensure user authenticity.

Procedure	Begin
	GenerateKeyPair();
	ReceiveMessageFromBA();
	Module I: Generation of Cipher Text C
	1. getInstance("AES");
	2. Extract each 16 bits of Message M
	3. For each 16 bits of the message,
	loop
	a. Encrypt(M,PrivateKey);
	b. AppendtoCipher(C,E(M));
	end loop
	4. Return Cipher Text C to the Caller.
	Module II: Generation of Message Digest
	1. getInstance("SHA256");
	2. CreateDigest(M,Key);
	3. Return Message Digest MD to caller
	Module III: Generation of Digital Signature
	1. ReadMessageDigest();
	2. getInstance("ECDSA");
	3. CreateSignature(MD,Key);
	4. Return DigitalSignature DS to the caller.
	End

5.3 Implementation of Central Database Agent

The algorithm implementing the Central Database Agent (CDA) functionalities is shown in table 3.

Table 3: Algorithm for implementation of Central Database Agent Functionalities

Algorithm	Implementation of Central Database Agent Functionalities.
Input	New Hotel Registration Details, Existing Hotel Information Update Details.
Output	Up-to-date Information of Hotels in Central DB

Procedure	Begin
	ReceiveRequestFromUA();
	ConvertRequestToQuery();
	OptimizeQuery();
	If (request = "New Hotel Registration")
	DisplayHotelRegistrationForm();
	UpdateCDB(); //CDB – Central Database.
	SendAckToUA();
	Else if(request = "Hotel Search")
	SearchCDB(query);
	SendResponseToUA();
	Else if(request = "Hotel Info Update");
	ReadHotelId();
	DisplayHotelInfoUpdateForm();
	UpdateCDB();
	SendAckToUA();
	End if;
	End;

The snapshots in figures 6 depict CDA (Central Database Agent) in action.

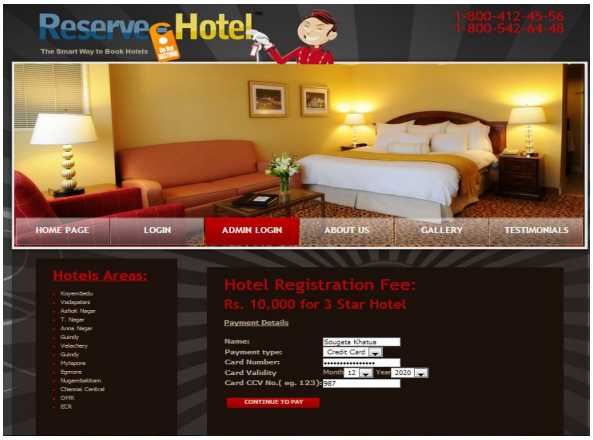

Fig 6. New Hotel Registration Fee Details

5.4 Implementation of Booking Agent

The algorithm implementing the Booking Agent (BA) functionalities is shown in table 4.

Table 4: Algorithm for implementation of Booking Agent Functionalities

Algorithm	Implementation of Booking Agent Functionalities.
Input	Users' Request for Hotel Booking / Cancelling already made Booking
Output	Receipt for Booking / Acknowledgement for Cancellation
Procedure	Begin

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

	ReceiveRequestFromUA();
	ConvertRequestToQuery();
	OptimizeQuery();
	If (request = "Booking Request")
	ReadPaymentDetails();
	SendPaymentDetailsToSA();
	ReceiveBookingReceiptFromSA();
	SendReceiptToUA();
	Else if(request = "Cancel Request")
	ReadReceiptDetails();
	SendDetailsToSA();
	ReceiveAckFromSA();
	SendAckToUA();
	End if;
	End;

The snapshots in figure 7 depicts the functionalities of Booking Agent.

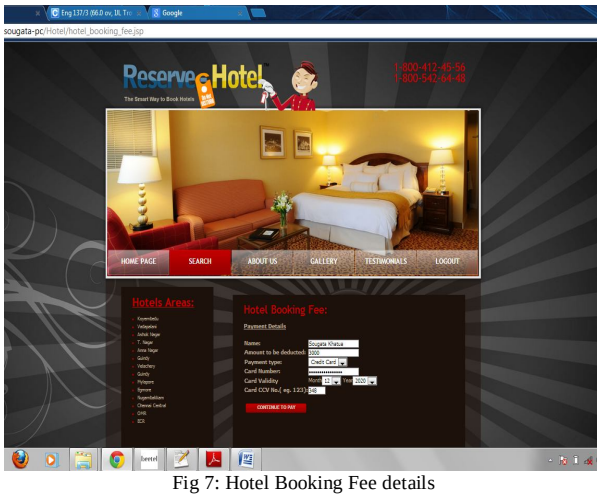

Fig 7: Hotel Booking Fee details

5.5 Implementation of Card Agent (CA)

The algorithm implementing the Card Agent (CA) functionalities is shown in table 5.

Table 5: Algorithm for implementation of Card Agent Functionalities

Algorithm	Implementation of Card Agent Functionalities.
Input	Encrypted Message, Message Digest, Digital Signature
Output	Verification result of users' authentication, message integrity and booking receipt / acknowledgement for cancel booking.

Procedure	Begin
	ReceiveSecuredMessageFromSA();
	VerifyAuthenticity();
	VerifyMessageIntegrity();
	DecryptMessage();
	ReadRequest();
	If (request = "Booking")
	SendCardDetailsToCCDC();
	//Credit Card Data Center
	ReceiveResponseFromCCDC();
	GenerateReceiptInfo();
	EncryptMessage();
	SendEncryptedMessageToSA();
	Else if(request = "Cancel Booking")
	ReceiveReceiptDetailsFromSA();
	ProcessRequest();
	EncryptResponse();
	SendEncryptedAckToSA();
	End;

6. Measurement of Quality and Reliability

The source code of implemented agent based Secured Online Hotel Booking System (SOHBS) is measured by the Halstead's Software Science [19].

The source code is measured in terms of program size, development effort and development cost of the software. The measurable and countable properties are:

- n_1 - Number of distinct operators
- n_2 - Number of distinct operands
- N_1 - Total number of operators
- N_2 - Total number of operands

From these metrics Halstead defines,

1. *Program Length:* $N = N_1 + N_2$
2. *Program Vocabulary*: $n = n_1 + n_2$
3. *Estimated Length:* $N = n_1 \log_2 n_1 + n_2 \log_2 n_2$
4. *Program Volume* $V = N \log_2 (n_1 + n_2)$
5. Difficulty: $D = (n_1 / 2) * (N_2 / n_2)$
6. *Effort:* $E = V * D$
7. *Time to Understand / Implement (sec):* $T = E/18$

These measurements help to:

- Predict an error
- Predict maintenance effort
- Measure overall quality of the program
- Measure overall reliability of the system

Hence, these measurements are used to enhance the reliability and quality of the software.

7. Performance analysis

After completion of implementation phase, the performance of the proposed agent based Secured Online Hotel Booking System (SOHBS) is analyzed under various circumstances.

7.1 Analysis of Security Algorithms

7.1.1 Analysis of Symmetric key Algorithms

The AES symmetric key algorithm is used for encryption and decryption purpose because AES is encryption standard specified by National Institute of Standards and Technology (NIST). Besides this, AES has many advantages which are discussed below.

The performance of AES i.e. Rijndael is compared against RC2, DES and Tripple DES symmetric key algorithms [20]. The performance of AES is compared with these

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

algorithms under various conditions to prove that AES is better than other algorithms and that's why AES is used in the proposed agent based Secured Online Hotel Booking System (SOHBS) to provide the security for confidential messages.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with 3GB RAM, Windows 7 using Java Cryptography Package.

The comparison is illustrated in figure 8 and figure 9.

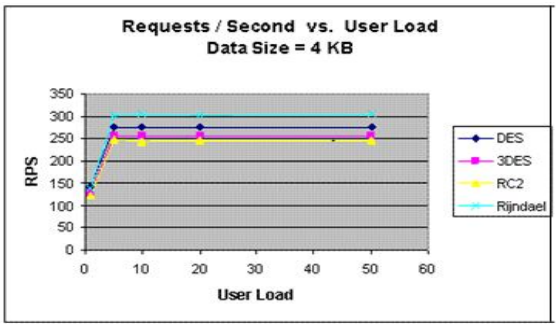

Fig 8. Request per second Vs User Load

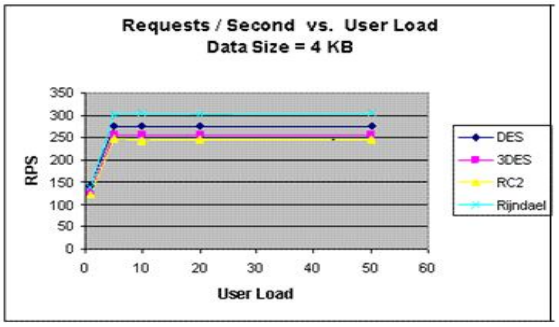

Fig 9. Response time Vs User Load

The results show that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

7.1.2 *Analysis of Asymmetric Key Algorithms*

The performance of Elliptic Curve Digital Signature (ECDSA) which is based on Elliptic Curve Cryptography (ECC) is analyzed against RSA, Elgamal and Digital Signature Algorithm (DSA). The key size details are illustrated in table 6.

Table 6. Key size details [21]

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	

The key sizes shown in table 6 are specified by NIST. These are standards. From the table it is clear that ECC has much less key size compared to other algorithms. So it is much faster than other asymmetric key algorithms. ECC-192 is used in the proposed hotel booking system for integrity and authentication.

In the proposed system, the combination of ECDSA and SHA-256 hash function is used to provide integrity service. Here SHA-256 is chosen because there is no major attack reported against it and it is used with ECDSA to increase its strength.

To compare the performance of the signature generation process and verification process, SHA256 with ECDSA and SHA256 with RSADSS are used.

Platform: Intel Core 2 Duo processor @ 2.2 GHz with Windows 7 using Java Cryptography Package.

The comparison table for performance analysis is given in table 7.

Table 7. Performance analysis of signature generation and verification process

Digital Signature Scheme	Key generation	Signature generation	Signature verification	Total time
SHA256 with ECDSA	0.5 sec	0.7 sec	0.8 sec	2.0 sec
SHA256 with RSADSS	1.1 sec	0.8 sec	0.6 sec	2.5 sec

Graph chart of execution time:

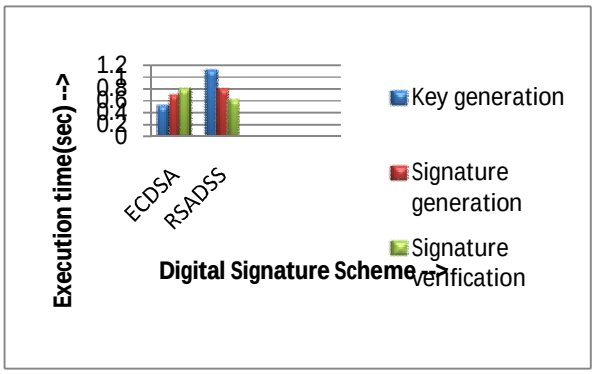

Fig 10. Graph chart of execution time of digital Signature schemes

From the Table 7 and Figure 10, it is clear that ECDSA is faster than RSADSS and also the key size ratio of the ECDSA is much less than the RSADSS. Hence the performance of the ECDSA is much is much ahead of RSDSS.

7.2 Analysis of the proposed agent based Secured Online Hotel Booking System (SOHBS)

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

The performance of the proposed agent based Secured Online Hotel Booking System is analyzed against 50 concurrent users. Hence up to 50 users can easily use the system without any problem.

7.2.1 Page Duration

The Page Duration chart shows the minimum, maximum and average page duration for all pages in the test relative to the elapsed test time (sample period) in which they completed. The page duration includes the time required to retrieve all resources for the page from the server. It includes network transmission time but not browser rendering time.

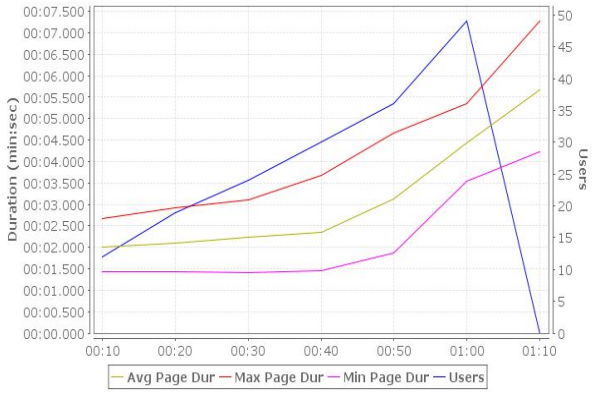

Fig 11. Analysis of Page Duration

From the load testing, it is determined that the page duration remains far below which is shown in the figure 11. So the proposed system is a well performed system.

7.2.2 Bandwidth Consumption:

The Bandwidth chart in figure 12 shows the total bandwidth consumed by traffic generated directly by the load test engines throughout the test relative to the elapsed test time (sample period). The bandwidth consumption is described in terms of the servers; i.e. outgoing bandwidth refers to data sent by the server to the browser.

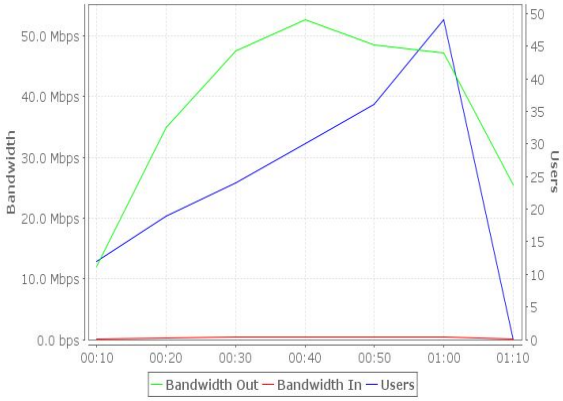

Fig 12. Bandwidth Consumption

The maximum bandwidth is consumed when the number of user reached 50 which is also pretty much under control. Hence the consumed bandwidth is under control and performance is also good.

7.2.3 Waiting Users

The Waiting Users and Average Wait Time metrics help diagnose certain types of performance problems. For example, they can help determine what pages users have stopped on when a server becomes non-responsive. The 'Waiting Users' metric counts the number of users waiting to complete a web page at the end of the sample period. The 'Average Wait Time' describes the amount of time, on average, that each of those users has been waiting to complete the page.

Fig 13. Waiting Users

From the figure 13, it is clear that the average wait time is pretty less. It is always remain below 2 minutes 50 seconds which is not the case for other systems.
Hence from the above discussion, it is clear that the proposed agent based Secured Online Hotel Booking System (SOHBS) performs better in all aspects of security and performance than the existing hotel booking systems.

8. Conclusion and Future Work

With the advancements in Internet and e-commerce technologies, the users wish to have reservation of the hotel rooms of their choice without any human intervention. This requirement of the users triggers the automation of hotel booking process over the Internet and provides more personalized information services for customers. The above analysis suggests that the Agent based Secured Online Hotel Booking System performs better than the existing hotel booking systems.

In future we can use *Hyper Elliptic Curve Cryptography (HECC) instead of using ECC.* Now many mathematicians are analyzing it and this algorithm needs only 80 bit long key to achieve the required level security. So it will need less key size than ECC. So, in future, when the security packages will be available for this algorithm, this algorithm can be implemented to enhance the security and performance of the system.

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.

Acknowledgments

I, Jaya Subalakshmi R., remain thankful to Dr. Margret Announcia, Dean, School of Computing Science and Engineering, VIT University, Vellore, for her immense support and motivation given for carrying out this work.

References

[1] 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, 2008,pp.37-49.

[2] 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", http://ww1.ucmss.com/books/LFS/CSREA2006/EEE4609.pdf

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

[4] Rust, R. T., and Kannan, P. K. "E-service: A New Paradigm for Business in the Electronic Environment," Communications of the ACM, 2003, Vol 46, No 6, pp. 37-42.

[5] Luck, M., McBurney, P., Preist, C., "Agent Technology: Enabling Next Generation Computing (A Roadmap for Agent Based Computing)", Agent Link, 2012.

[6] Fabio Luiqi Bellifemine, GovanniCaire and Dominic Greenwood, " Developing Multi-Agent Systems with Jade", John Wiley Sons Ltd,England, 2007.

[7] N. Sivakumar, K. Vivekanandan, B. Arthi, S.Sandhya, Veenas Katta, "Incorporating Agent Technology for Enhancing the Effectiveness of E-learning System", IJCSI International Journal of Computer Science Issues, Vol 8, No 1, 2011, pp 454-460.

[8] S. Srinivasan, Jagjit Singh and Vivek Kumar, " Multi-agent based decision Support System using Data Mining and Case Based Reasoning", IJCSI International Journal of Computer Science Issues, Vol. 8, No 2, 2011, pp. 340-349.

[9] Pooja Jain and Deepak Dahiya, "An Architecture of a Multi Agent Enterprise Knowledge Management System Based on Service Oriented Architecture", IJCSI International Journal of Computer Science Issues, Vol. 9, No 3, 2012, pp 395-404

[10] Courtney McTavish, Suresh Sankaranarayanan, "Intelligent Agent based Hotel Search & Booking System", International Conference on Electro/Information Technology (EIT), 2010, pp.1-6.

[11] Qi Wei, Catherine Cheung and Rob Law, "Tourist Perception of Online Hotel Bookings, International Conference on E-Business and E-Government,2010, pp. 2273 – 2276.

[12] Hongyun Kuang and Jie Yang, "Empirical Analysis on Hotel Online Booking Consumer's Satisfaction with E-service of Website", International Conference on Information Management, Innovation Management and Industrial Engineering, 2011,Vol 1, pp. 193-196.

[13] Shazia Yasin, Khalid Haseeb and Rashid Jalal Qureshi, "Cryptography Based E-Commerce Security: A Review", IJCSI International Journal of Computer Science Issues, Vol. 9, No 1, 2012, pp. 132-137.

[14] Vineeta Khemchandani and Prof G.N.Purohit, "Information Security and Sender's Rights Protection through Embedded Public Key Signature", IJCSI International Journal of Computer Science Issues, Vol. 7, No 9,2010, pp 27-34.

[15] Mark S. Ackerman and Donald T. Davis, Jr., "Privacy and Security Issues in E-Commerce", Review chapter for the New Economy Handbook (Jones, ed.).

[16] Wayne Lawrence, Suresh Sankaranarayanan, "Application of Biometric Security in Agent based Hotel Booking System - Android Environment", I.J. Information Engineering and Electronic Business, Vol-3, 2012, pp: 64-75.

[17] A. Kannammal, N. Ch.S.N. Iyengar, "A Framework for Mobile Agent Security in Distributed Agent-Based E-Business Systems", International Journal of Business and Information, Vol 3, No 1, 2008.

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

[19] http://en.wikipedia.org/wiki/Halstead_complexity_measures

[20] D.S.Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Vol 8, No 8, 2009, pp. 58-64

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

R. Jaya Subalakshmi is an Assistant Professor (Junior) in the School of Computing Science and Engineering at VIT University, Vellore, Tamil Nadu, India. She did M.Sc in Computer Science and Currently pursuing M.S.(By Research) in VIT University. Her research area is Cryptography, Data Privacy and Agent based Distributed Computing.

Dr. N.Ch.S.N. Iyengar (M.Sc, M.E, Ph.D) is a Senior Professor in 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 136 research Publications in International Journals. He chaired many international conferences and delivered invited/ technical lectures/ keynote addresses besides being International programmed committee member.

Sougata Khatua has received his B.Sc (Computer Science) degree from Midnapore College under Vidyasagar University, Paschim Medinipur , West Bengal, India. He pursued M.Sc (Computer Science) at VIT University, Vellore, Tamil Nadu,India. His areas of Interest are Intelligent Distributed Computing, Cryptography and Information Security.

Haleema (M.C.A., M.Phil,, M.Tech) is an Assistant Professor (Senior) in the School of Social Science and Languages and pursuing her Ph.D. research work in the School of Computing Science and Engineering. Her area of research is Security in Cloud and Distributed Systems.

Copyright (c) 2013 International Journal of Computer Science Issues. All Rights Reserved.