Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI-AGENT SECURITY ARCHITECTURE FOR A SHARIA COMPLIANT E-AUCTION

[1]NOR AIMUNI MD RASHID, [2]NORLEYZA JAILANI, [3]ROSSILAWATI SULAIMAN, [4]ZURAIDAH ABDULLAH

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor MALAYSIA

E-mail: [1]aimuni.rashid@gmail.com, [2]njailani@gmail.com, [3]rossilawati.s@gmail.com, [4]zuraidahabdullah56@gmail.com

ABSTRACT

Electronic auction has introduced new processes in the way auction is conducted which require investigation to ensure compliancy to Sharia (Islamic principles that are based on Qur'an and Sunnah) rules. The use of mobile software agent in electronic auction marketplaces adds ubiquity power to the bidders. In particular it allows agents to quicker respond to local changes in auction marketplaces and make bidding strategy decisions faster than remote agents or human participants could. Nevertheless, mobile agent raises issues concerning malicious attacks from a variety of intervening sources that might alter the sensitive information it carries. A multi-agent based e-auction must fit the concept of halal trade and address the problems resulting from fraud activities in online auction. Most auction frauds such as bid shilling and bid shielding also violate Sharia transaction law. If an attacker gains information on sensitive data such as the maximum bid for the bidders, the information can be manipulated to artificially increase prices through bid shilling. A Sharia compliant e-auction must comply with Islamic business law and offer secure and trustworthy trading environment. This paper discusses findings of non-compliances to Sharia rules found in the case studies conducted on a number of major online auction systems. This paper focuses on addressing the bid shilling problem by proposing multi-agent security architecture for Sharia compliant e-auction which encompasses security protocols for mobile agent authentication and confidentiality of sensitive information. Mobile agents are used to carry bidders' and sellers' data. Cryptography protocol such as encryption/decryption, digital signature and hash function are used and applied on identified high and low risk data.

Keywords: *E-Auction, Security, Cryptography, Multi-Agent, Sharia Compliant*

1. INTRODUCTION

Online or electronic auctions (e-Auctions) provide numerous advantages including scalability, flexibility, fast searching, and cost minimization. Unfortunately, online auctions also have the disadvantages of higher fraud risk and manipulation [1]. Criminals are attracted by the low entry costs and tremendous profits of Internet auctions. eBay for example reported that revenue for the fourth quarter ended December 31, 2013, increased 13% to $4.5 billion, compared to the same period of 2012 [2]. Although revenue generated through online auctions is competitive, fraud activities in online auctions is the most common type of fraud reported amongst internet crime [3]. Using mobile agent in online auctions adds to the complexity of the security problems. Thus many research efforts have been carried out to address these problems due to the intricacy of the security and trust issues and its significance to businesses.

This paper is organized in four main sections. The second section provides related work which includes issues of non-compliancy to sharia rules, frauds, security and state-of-the-art of security mechanism in mobile agent system. In the third section, requirements for Sharia compliant online auction are discussed. We also propose a new multi-agent Sharia compliant architecture. Section four describes the security protocol that supports the proposed architecture. The last section focuses on discussion, conclusion and direction for future works.

2. RELATED WORKS

While Islamic banking and financial services are gaining reputation and becoming the subject for

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

research in the area of service science [4] and Service Oriented Architecture (SOA) [5], the issue of non-compliancy of e-auction to Sharia principles has not been explored. In Islamic business practice traditional auction termed as "al-Muzayadah" meaning "the increase" was accepted as legal during the time of the Prophet Muhammad (PBUH). In Oman auction system is still in practice until today to distribute water supply in irrigation system to farmers [6]. However the conversion of traditional auction to online auction raises new questions such as the legality of the transactions and the legitimacy of the contract and its transaction [7]. In other words the issues of whether the e-auction transactions are sharia-compliant have not been addressed adequately.

2.1 Non-Compliancy of e-Auction to Sharia Rules

Islam urges for two preliminary principles of permissibility and harmlessness when doing their daily business either electronically or in conventional way [8]. Permissibility meaning fully compliant with Islamic norms and harmlessness emphasize that no harmful implications for others or the public. Studies indicated that some electronic auctions are not Syariah compliant hence Muslim users are exposed to prohibited features like riba (interest), maisir (gambling), gharar (uncertainty) and najash (articially inflating price) [9, 10]. The International Fiqh Council published its decision on auction contract either offline or online which stated the contract's validity under the conditions that the underlying transactions including administration, management, and control must be compliant with Sharia [10]. Specifically the resolution suggests the following conditions must hold true:

• Auction organizer or seller is allowed to request assurances from any auction participants to ensure that all potential buyers are true and commit to the purchase should they win the auction.

• Authorized auction organizer is allowed to charge participants, provided it does not exceed the actual value. (Meaning that it must be the minimum for the purpose of operational and administration only).

• Seller or promoter is banned from advocating false-bid to increase the price. Other form of Najash is that expert who is non-participant praising the quality of an item so that other bidders raise the price up, when in reality the appraisal comes from the seller.

• Sellers and their partners cheating the market price, by saying that the so-called item are on sales.

• Sellers promote high quality products that can be read, heard and seen to raise prices when in reality it is not.

Unfortunately, very few publications discuss online auction from the jurists' point of view. Abd Rahman [10] briefly discussed the auctioning mechanisms in eBay (eBay.com) and swoopo (www.swoopo.co.uk). From his personal experience he concluded purchasing items via eBay auction is permitted as long as the above conditions are fulfilled. This holds true except for buying gold, silver and currency. Selling on eBay is also permissible, and commission taken by PayPal and eBay from buyers is also allowed as it is considered service charge for a specific task. However the calculation and amount must be made known at the beginning of the transaction. Receiving payment from buyers using conventional credit card is also permissible as it is beyond the seller's control and responsibility. However, paying through a conventional credit card is illegal, even if the buyer pays the price 'on time' to the card issuer, it is because each purchase will give commission to the credit card issuer, it will be considered to directly contributing to the development of the riba credit card industry. Payment via PayPal depends on the card associated to PayPal which is a credit, debit or charge card. If it is a card issued by conventional bank, payment through PayPal is also illegal. The duration for goods delivery and the approximate date the good will reach the buyer must be revealed to the buyer. Warranty must be publicized or seller can be contacted if the goods are not delivered pass the promised date. For damage or dishonor guarantee, what makes eBay reliable is the fact that eBay gives compensation if goods are damaged or the seller do not honor the transaction. In one incident a buyer receives compensation when the television bought through eBay has damage which is not clearly stated by the seller in sales specifications. Such action and provisions from eBay makes the gharar become smaller and fall in the category of gharar yasir (less uncertainty) which can be excused. Meanwhile bidding in Swoopo is prohibited since buyer is required to pay for the rights to bid. Each time a bid is placed, the 40 pence will be deducted from the user account. This is similar to gambling whereby paying bid rights is

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

equivalent to betting, and the good sold is considered the winning trophy. Other bidders who lost will lose the money used to pay for each bid.

Al-Munajjid [11] differentiated between credit and debit cards in which the former is illegal while the latter is legal. When exploring eBay and bidz (www.bidz.com), Al-Munajjid [12] reached to the same conclusion with regards to trading jewelry as [10]. Other than jewelry, trading is lawful unless fraud or other prohibited activity is detected. However, those studies investigate the studied sites in a broad sense but never go deeply to discover the underlying prohibited activities as being discussed in [9]. Using four rounds of Delphi technique with a panel of Sharia experts from Universiti Kebangsaan Malaysia, Jamalludin et al. [9] identified eight features that are to some extent inconsistent with Islamic Sharia principles. Forms of prohibited processes such as najash (prices inflation), gharar (uncertainty), riba (Interest), and maisir (gambling) have been identified.

Table 1 shows the Sharia requirement features that should be present in a Sharia compliant e-auction. Issues mostly are related to auction procedures in which some Sharia violations are detected. Firstly, service charges for auction, bid or delivery must comply with Sharia rules. The auction fees in most conventional e-auction systems are not precisely defined at fixed values while interest i.e. riba is detected in many cases. For instance, auction fee in some sites is defined as percentage from the winning price.

In Islamic business rules, any service can be defined under the concept of Ijarah where fees must be previously defined and agreed by both parties. Bid fee is allowed to be taken but only for guarantee purpose and not to be taken as auction revenue. Therefore, Sharia rules urges that bid fees are refunded to all losing bidders and subtracted from the price a winner has to pay. In case the winner does not pay the due price then the seller has the rights to confiscate the bid fee. Payment is another important issue since most e-payment methods such as PayPal do not comply with Sharia especially debit and credit cards because of many forms of interest taken. However, there are other payment methods that are almost compatible with sharia rules such as the use of Islamic debit and credit cards, direct bank transfer or bank cheque.

With regard to auction protocol there is no restriction either to bid in ascending or descending manner, sealed or open cry. It does not matter, as long as the bidder commits to the bidding amount. This implies that bid withdraw is unacceptable unless a satisfactory reason is declared. In order to avoid the prohibited uncertainty (Gharar), seller has to declare accurate auction losing rules. In most conventional e-auctions, the closing rule is predefined threshold timing when auction must be closed and then the auctioneer shall announce the winning bid. Due to some security challenges such as sniping and bid shielding, some auction site such as Yahoo sometimes allow for time expansion which is considered from Islamic perspective as a cause of uncertainty. Therefore the best solution is auction time must not be allowed to be extended. Another important requirement is the winning determination rule which must be stated clearly beforehand to avoid bidder uncertainty. For instance in ascending auction the highest price might not be the only attribute being considered to winning the auction but also a degree of trust or bidder location. Furthermore, sharia requires seller's consent to accept the highest bid or another acceptable bid from his perspective. Such consideration clearly comes in contradiction to conventional e-auction systems which automatically consider the highest bidder is the winner despite seller dissatisfaction.

Table 1: Sharia Requirements for e-Auction

Issue	Sharia Requirement
Identity	- Eligibility in terms of age and free will - True Names - Accurate Information
Product	- Adequately described - Permissible i.e. Halal - Owned by seller (ownership certificate)
Auction Fees	- Comply with Ijarah rules: fixed amount, pre-agreed, & precisely defined - Paid by seller only - Refunded if auction fails
Bidding fees	- Comply with Ijarah rules: fixed amount, pre-agreed, & precisely defined - Defined for all bidders equally - Refunded to all losers - Subtracted from winning price
Payment Method	- Fixed annual rates - Free or fixed amount per transaction - Rates comply Ijarah rules
Bid withdraw	Not allowed for winner
Closing rule	- Auction end in timing threshold - End time not allowed to be expanded
Determining winner	- Winning attributes clearly stated - Auction protocol set by seller - Seller consent necessary (must satisfied with price)
Delivery	- Independent contract from auction contract. - Charges must be clearly set - Guarantee product return

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Issue	Sharia Requirement
Selling Contract	Established after the seller determines winning bid

2.2 Frauds in e-Auction

Usually, e-auction involves four stockholder entities including seller, bidder(s), auctioneer, and the sold item(s). Unscrupulous sellers take advantage of buyers by misrepresenting the quality or condition of their goods. Some have no intention of delivering the goods that are offered for sale. Bid shilling is one of the hardest types of online auction fraud to detect and is considered as an example of criminal fraud in the US and other parts of the world and in the most severe cases punishable by a jail term or heavy fines [13]. Shilling occurs when a seller bids on her own auction in an effort to increase the price other bidders need to pay to win the auction. This is an instance of Najash. In this case have, the final bidder is motivated to shave some surplus off the highest bidder by making that final bidder pay more. In contrast there are other motivations for shilling such as to avoid paying auction house fees. Online auction houses, like eBay, typically charge a fee that is determined by the amount a seller sets for the initial bid, while bidding is typically free. By setting a low starting bid price, and then secretly bidding that amount up by pretending to be a bidder, sellers can save money when selling goods in online auctions. This is known as reserve price shill bid. Furthermore, the chance of detection is low, since the names and faces of the actual bidders are hidden from the other bidders, unlike a typical traditional live auction where everyone can see who is bidding. Kauffman and Wood [13] describe how a premium bid, a bid which is higher than other bids for the same item in different auctions, is often a reserve price shill bid. Bid shielding occurs when a buyer and a partner (not a seller) artificially inflate the bids, discouraging others from bidding. Then, at the last minute, the shielder cancels his high bid and allows his partner to win the auction with a lower bid [14]. This will decrease seller's profit. Furthermore, many users describe their online auction experience as comparable to gambling. The issues of *najash* (artificially inflating price) in auction process should be resolved to regain trust among the Muslim users. Our proposed protocol will address and focus on bid shielding problem to fulfill the needs of Sharia compliant requirement in e-auction marketplace.

2.3 State-of-the-art of Mobile Agent Security

The growing number of research efforts in the areas of mobile e-commerce agents [15] and agent-mediated e-commerce [16,17,18] testify the potential benefits of integrating mobile agents in more advanced e-commerce applications such e-auction system raises many new security issues that are quite different from conventional client/server systems. Auction server which accommodates the agents can be attacked by malicious agents. Similarly agents could be carrying sensitive information about their owners and should be protected from tampering by malicious hosts. There is a need to improve the security and privacy throughout the auction process. Security ensures that agents are protected from malicious attacks during transportation and bidding. Meanwhile, privacy is provided to protect sensitive information such real identity of each participating bidder with encryption mechanism [19]. Although agents may simplify many auction processes, many security problems have yet to be solved specifically with regards of fraudulent behavior posed by both agents and human in online auctions. Table 2 (at the end of the paper) compares the security measures deployed by mobile agents in various works. In summary, multi-agent system allows sensitive data to be transferred between nodes, thus addressing security issues such authentication, confidentiality, integrity and access control. Therefore it can be considered as a good paradigm to perform secure data transaction. To date various techniques have been proposed for securing mobile agent and its data from malicious entities. In general, AES is widely used for the encryption of large size from the year 2001, while RSA is used for encrypting and distributing symmetric key (AES) who's size is very much smaller than the data. Our proposed protocols also use AES algorithm and RSA for controlling AES key distribution.

3. PROPOSED SECURITY ARCHITECTURE

In an agent-based online auction participating agents play a specific roles defined by the auction framework. Most common agent involved in auction marketplace are bidder agent, supplier agent or seller agent, broker agent, coordinator agent, auctioneer agent and third party agent [19,20]. Figure 1 shows the proposed security architecture of a mobile agent-based e-auction system with a Halal trade Agent responsible to

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ensure all transactions and processes comply with Sharia rules and regulation. This agent will be implemented as a normative agent [21] in future work. This architecture is based on our previous work which proposed a conceptual framework for mobile agent-based halal marketplace [22]. For initial implementation, it has been simplified to include only Buyer Agent, Seller Agent, Guard Agent, Certificate Authority, Registration Authority, Directory Service, Auctioneer Agent, Auction Handler, Event Logger and Auction Database.

Buyer agent is mobile agent created on behalf of a user buyer when he decides to enter the auction market to bid for a specific item. It carries owner's certificate, unique ID, owner information, product/services request, account information, etc. Seller agent carries certificate, unique ID, owner information, bid indication, product/services offered, certificate of ownership, etc. The Certificate Authority acts as a Trusted Third Party (TTP) which acknowledges the validity of the public keys, issues digital certificates auction participants as a proof of identity and provide necessary information for authentication between trading parties.

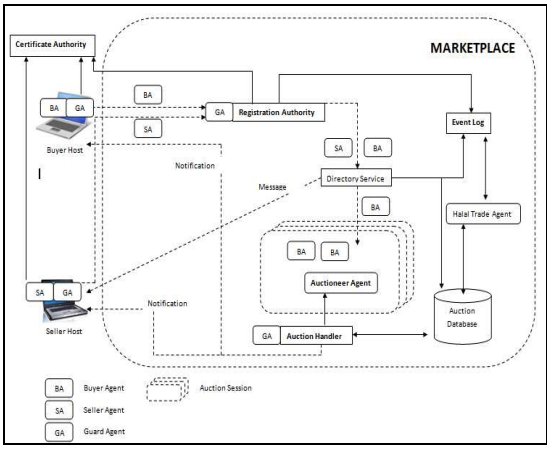

Figure 1 : Security Architecture of a Sharia Compliant e-Auction

Guard Agent performs mobile agent authentication before it moves to enter/exit the auction market. Registration Authority handles registration with the auction market. Directory Service registers items offered by Seller Agent into Auction Database. Auction Handler creates Auctioneer Agent to host auction for each product/service for the duration time specified by Seller Agent. Directory Service is also for publishing products/services offered by Auctioneer Agent(s). All events associated to agent and transaction will be logged in Event Logger. Detailed explanation of the system architecture is available in [23]. The following section will describe the security protocols for securing the mobile agent in the auction process.

4. PROPOSED SECURITY PROTOCOL

Figure 2 depicts the notation and flow of processes that take place in the protocol for protecting bid information carried by bidding agent. The security protocol is adapted from [7]. This protocol is used for authenticating mobile buyer and seller agents during its transmission from user device to auction market. The protocol assumes mobile agent (MA) trusts initiator (I), responder (R) and MA trust Certificate Authority, and all other parties do not trust each other.

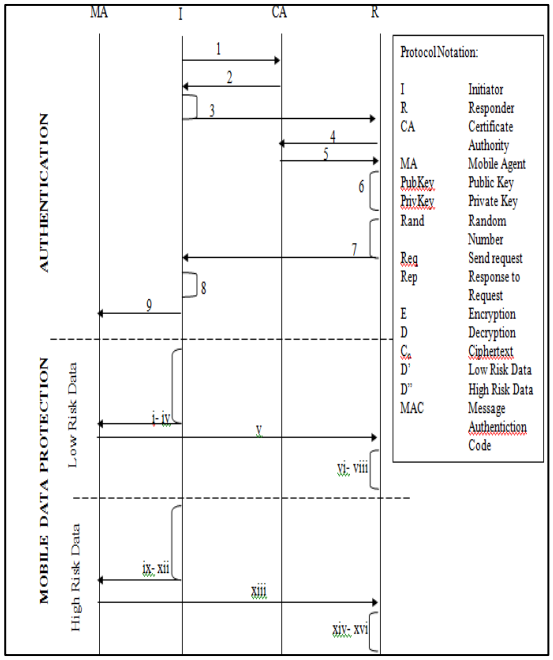

Figure 2 : Security Protocol for Mobile Bidding Agent

The security protocol will be divided into 2 phases namely Authentication and Mobile Data Protection.

4.1 Authentication

The authentication process takes place before the mobile agent was send to the marketplace. Sender must be authenticated by the registration authority before any transportation of mobile agent is made.

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This phase involved two parties, the sender Guard agent that act as the initiator and Registration Authority's Guard Agent as the responder.

1. Initiator send request to the certificate authority for the Responder public key.

$$\text{Req}_I\ (PubKey_R)$$
$$I \dashrightarrow CA$$

2. Certificate Authority issues the PubKey_R to the initiator

$$\text{Rep}_{CA}(PubKey_R)$$
$$CA \dashrightarrow I$$

3. Generates a random number, $Rand_I$. Encrypts $Rand_I$ using PubKey_R to produce a ciphertext and dispatch it to the Responder.

$$C_1 = E_I\ (PubKey_R, Rand_I)$$
$$I \xrightarrow{C_1} R$$

4. Upon received the C_1 from the initiator, Responder send request to the certificate authority for $PubKey_I$.

$$\text{Req}_R\ (PubKey_I)$$
$$R \dashrightarrow CA$$

5. Certificate authority issues the $PubKey_I$ to the Responder

$$\text{Rep}_{CA}\ (PubKey_I)$$
$$CA \dashrightarrow R$$

6. Responder performs the decryption process to gain the initiator $Rand_I$ using $PrivKey_R$

$$D_R\ (PrivKey_R, C_1\ ) = Rand_I$$

7. Responder generates $Rand_R$. Encrypt $Rand_I$, and $Rand_R$ using $PubKey_I$ to produce second ciphertext, this ciphertext will then send to Initiator.

$$C_2 = E_R\ (PubKey_I, Rand_I, Rand_R\ )$$
$$R \xrightarrow{C_2} I$$

8. Once the C2 arrived at the initiator side, the initiator will perform decryption process to retrieve the $Rand_s$, and $Rand_R$ using its $PrivKey_I$. Initiator verify the $Rand_I$

$$D_I\ (\ PrivKey_I, C_2\ ) = Rand_I, Rand_R$$
$$\text{Verify}_I\ (Rand_I)$$

9. Copy the $Rand_R$ into MA.

$$\text{Copy}_I\ (\text{Rand}_R, MA)$$

Thus the secure connection between initiator and responder had been established.

4.2 Mobile Data Protection

For buyer agent, the data will be divided into two categories high risk data (D") and low risk data (D'). The high risk data are maximum offer and bid increment value. Meanwhile low risk data are email, phone number, product chosen, product brand and product model. For Seller agent, the data that will be encrypted are name, company registration number, email, phone number, product offered, minimum price, auction close time, and shipping fee.

For both buyer's low risk data and seller agent's data, the encryption process as follows:

i. Initiator generate a secret key, K_I

ii. Initiator encrypts the data with K_I to produce a ciphertext C.

$$C_1 = E\ (D', K_I)$$

iii. Initiator computes the Message Authentication Code (MAC) using generated MAC key *MacKey* and C_1. MAC used to identify whether the ciphertext had been tempered or not.

$$MAC = \text{compute}\ (\text{MacKey}, C_1)$$

iv. Initiator encrypt K_I, *MacKey*, *MAC* and responder random number (from section a.9) to produce a cipherkey, CK using the responder $pubKey_R$.

$$CK = E(K_I, MacKey, MAC, Rand_R, pubKey_R)$$

v. Both C_1 and CK carried by sender mobile agent to the responder

$$I \xrightarrow{C_1, CK} R$$

vi. Upon arriving, responder decrypts the CK to gain access to the keys, using its $privKey_R$.

$$MacKey, MAC, Rand_R = D(CK, privKey_R)$$

vii. First the responder will verify the carried $Rand_R$ with its own $Rand_R$. If the $Rand_R$ is valid, responder will compute MAC using *MacKey*, and the C_1. After that, responder will verify the new generated MAC and MAC carried by the mobile agent are valid

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

or not. If it's valid means that C_1 not tempered during the transportation.

$Verify_R = (Rand_R)$
$VerifyR = (MAC)$

viii. Responder decrypt C_1 using decrypted K_1 to obtain the carried data for the database update purpose.
$D' = D(C_1, K_1)$

For buyer agent high risk data, D", a separate encryption need to be done because decryption process will only occur at the bidding session.

ix. Encrypt the D" with a new generated secret key, K_2 to produce second ciphertext

$C_2 = E(D", K_2)$

x. Compute MAC using C_2 and K_2
MAC = compute(MacKey, C_2)

xi. Sign the C_2 with the initiator $privKey_I$.

$S = Sign(C_2, privKey_I)$

xii. Initiator encrypts K_2, *MacKey*, *MAC* and S to produce a cipherkey, CK using the responder $pubKey_R$. In this case the responder is auctioneer guard agent.

$CK_2 = E(K_2, MacKey, MAC, S, pubKey_R)$

xiii. Both C_2 and CK carried by sender mobile agent to the registration Authority and once the mobile agent proceed to bidding session, auctioneer guard agent wills response as the responder.

C_2, CK
I ----------> R

xiv. Upon arriving at the bidding session, responder decrypts the CK to gain access to the keys, using its $privKey_R$.

$MacKey, MAC, S = D(CK_2, privKey_R)$

xv. First the responder will verify the carried *S* using initiator public key, $pubKey_R$. If the S is valid, responder will compute MAC using *MacKey*, and the C_2. After that, responder will verify the new generated MAC and MAC carried by the mobile agent to see its validity. If it is valid means that C_2 is not tempered during the transportation.

$Verify_R = (S)$
$VerifyR = (MAC)$

xvi. Responder decrypt C_2 using decrypted K_2 to obtain the carried data for the bidding process purpose.

$D" = D(C_2, K_2)$

5. DISCUSSION

Generally, for the mobile agent transmission from the users' host to the auction market or vice versa, both initiator and responder want to make sure that the data transferred is safe from any unauthorized access, meaning the data is not modified and non-repudiation can be proven. On the other hand, once the mobile agent safely arrives at the auction market, it must make sure the agent code is protected from being attacked by other agents. These requirements are identified as confidentiality, integrity and authenticity.

Consider a scenario where user A sends a bidder agent that carries a malicious code to discover other bidder's maximum bid offer. Agents can also work in collusion with each other to win over a bid. We have highlighted the issues of agents colluding with each other to inflate bidding prices (action of *najash*) if they are able to discover the highest price their opponent's is willing to offer. This information is vulnerable especially during mobile agent transmission from its user's host to the auction site. Users are also skeptical whether their agents are safe from attack by other agents while residing in a foreign machine that hosts the auction marketplace.

Hence we have designed the multi-agent security architecture of a Sharia compliant e-auction which encompass security protocols for mobile agent authentication and protection of sensitive bidding information. This architecture uses cryptography protocols to secure data and communication channel. To improve element of trust the architecture provides double encryption of high risk data which will only be decrypted before it starts to calculate bid offer.

In summary, this paper has identified necessary requirements for a Sharia compliant e-auction, presented system architecture and security protocol that addressed some security issues related to fraud

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in mobile agent-based e-auction. In our future work, we will discuss the results gathered from the implementation of the architecture and performances of mobile agents while carrying out the proposed security protocols.

REFRENCES:

[1] Lucking-Reiley, D. Auctions on the Internet: What's being auctioned, and how?. *The Journal of Industrial Economics*, 48(3), 2000, 227-252.

[2] http://finance.yahoo.com/news/ebay-inc-reports-fourth-quarter-211500331.html

[3] Kwan, M., Overill, R., Chow, K. P., Silomon, J., Tse, H., Law, F., & Lai, P. Evaluation of evidence in Internet auction fraud investigations. In Advances in Digital Forensics VI, 2010, 121-132.

[4] Javed, A., Masuda, H., & Kohda, Y. Value Analysis of Islamic Banking and Conventional Banking to Measure Value Co-creation. *International Journal of Social, Human Science and Engineering*, Vol. 8, No. 2. 2014.

[5] Jaafar, Ako A., and Dayang NA Jawawi. Integration Islamic Banking System Based on Service Oriented Architecture and Enterprise Service Bus in *Advances in Computational Science, Engineering and Information Technology*, 2013, 131-140.

[6] Al-Marshudi. A.S. The Falaj irrigation system and water allocation markets in northern Oman, *Agricultural Water Management* Vol. 91 issues 1-3, 2007, 71-77.

[7] Jailani, Norleyza, et al. Secure and auditable agent-based e-marketplace framework for mobile users. *Computer Standards & Interfaces* 30(4), 2008, 237-252.

[8] Zainul, Norazlina, Fauziah Osman, and Siti Hartini Mazlan. E-Commerce from an Islamic perspective. *Electronic Commerce Research and Applications* 3(3), 2004, 280-293.

[9] Jamalludin, S., Jailani, N., Ahmad, S., Abdullah, S., Mukhtar, M., Bakar, M. A., & Abdullah, Z. A Syariah compliant e-auction framework. *In International Conference on Electrical Engineering and Informatics (ICEEI)*, 2011, 1-6.

[10] Abd Rahman. Z. Law of Auction Buy and sell at eBay and Swoopo. Available at: *http://zaharuddin.net/pelaburan-&-perniagaan/793-hukum-jual-beli-lelong-di-ebay-a-swoopo.html*. 2008

[11] Al-Munajjid, M. Rulling on buying and selling on the bidz.com website. Available at: *http://islamqa.info/en/ref/142652. 2010*

[12] Al-Munajjid, M. Rulling in trading using eBay website. Available at: *http://islamqa.info/ar/ref/148591. 2010.*

[13] Kauffman, R. J., & Wood, C. A. The effects of shilling on final bid prices in online auctions. *Electronic Commerce Research and Applications*, 4(1), 2005, 21-34.

[14] Dolan, K. M. Internet auction fraud: the silent victims. *Journal of Economic Crime Management*, 2(1), 2004, 1-22.

[15] Kowalczyk, R., Braun, P., Mueller, I., Rossak, W., Franczyk, B., & Speck, A. Deploying mobile and intelligent agents in interconnected e-marketplaces. *Journal of Integrated Design and Process Science*, 7(3), 2003, 109-123.

[16] He, M., Jennings, N. R., & Leung, H. F. On agent-mediated electronic commerce. *IEEE Transactions on Knowledge and Data Engineering*, 15(4), 2003, 985-1003.

[17] Ito, T., Ochi, H., & Shintani, T. A group-buy protocol based on coalition formation for agent-mediated e-commerce. *IJCIS*, 3(1), 2002, 11-20.

[18] Neville. B. and Pitt. J. A computational framework for social agents in agent mediated commerce. *Engineering Societies in the Agents World IV*, 2004, 519-519.

[19] Sheng-Uei. G. An electronic auction service framework based on mobile software agents. *Encyclopedia of Virtual Communities and Technologies*, 2006, 179-187.

[20] Yi, X., Siew, C. K., Wang, X. F., & Okamoto, E. A secure agent-based framework for internet trading in mobile computing environments. *Distributed and Parallel Databases*, 8(1), 2000, 85-117.

[21] Ahmad, A., Mustapha, A., Ahmad, M. S., & Yusoff, M. Z. M. Analyzing The Principles of Islamic Jurisprudence for A Normative Framework in Multi Agent Systems. *International Journal on Quranic Research* (ISSN 2180-4893), 1, 2011, 51-72.

[22] Jailani, N., Patel, A., Yatim, N.F.M., Yahya, Y., Mukhtar, M., Abdullah, Z., Bakar, M.A., Othman, M. and Abdullah. S. A mobile agent based e-marketplace model for muslim community. *Proceedings of the International Conference on Knowledge Based Development* (ICKBD 2008), June 22-24 2008, 272-277.

[23] Rashid, Nor Aimuni Md, Norleyza Jailani, and Rossilawati Sulaiman. Security Architecture for Mobile Agent-based Shari'ah Compliant e-Auction Marketplace. *Procedia Technology 11,*2013, 510-517.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] Xiao-Long, X., Jing-Yi, X., & Chun-Ling, C. The model and the security mechanism of the information retrieval system based on mobile multi-agent. In *the 12th IEEE International Conference on (Communication Technology (ICCT)*, 2010, November, pp. 25-28.

[25] Sulaiman, R. and Sharma, D. Enhancing security in e-health services using agent. *International Conference on Electrical Engineering and Informatics*, 1-6 July 2011, 1-6

[26] Sulaiman, R., Huang, X., & Sharma, D. E-health services with secure mobile agent. *In Seventh Annual Communication Networks and Services Research Conference, 2009. CNSR'09*. 2009, May, 270-277).

[27] Subalakshmi, R. J., Das, A., & Iyengar, N. C. S. A small e-health care information system with agent technology. In *2011 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2011, October, 68-72).

[28] Ahmed, Tarig Mohamed. "Generate secure mobile agent by using SMS to protect Hosts." *IEEE/ACS International Conference on Computer Systems and Applications (AICCSA*), 2010, 1-4.

[29] P Vieira-Marques, P. M., Robles, S., Cucurull, J., Cruz-Correia, R. J., Navarro, G., & Marti, R. Secure integration of distributed medical data using mobile agents. *IEEE Intelligent Systems*, 21(6), 2006, 47-54.

[30] Shibli, A., Yousaf, I., & Muftic, S. MagicNET: security system for protection of mobile agents. *In the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 2010, April, 1233-1240.

[31] Marikkannu, P., Murugesan, R., & Purusothaman, T. AFDB security protocol against colluded truncation attack in free roaming mobile agent environment. In *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, 2011, June, 240-244.

[32] Geetha, G. and Jayakumar. C. Implementation of trust and reputation management for free-roaming mobile agent security. *IEEE Systems Journal*, 2014, 1-10.

[33] Wang Jing, and W. Shu yue. Identity Based Detecting protocol for mobile agent with onion itinerary. *Fourth International Conference on Multimedia Information Networking and Security*, 2012, 12-14.

[34] Srivastava, S. & Nandi. G.C. Fragmentation based encryption approach for self-protected mobile agent. *Journal of King Saud University-Computer and Information Sciences*, 26(1), 2014, 131-142.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Comparison of Mobile Agent Security Measures

References	Authentication	Confidentiality	Integrity	Access Control	Reliability
[24]**Focus:** Improve the performances of information retrieval systems. **Issues:** Fake malicious host, malicious mobile agents and fake information	Using X.509 certificates	Using SSL on the transport layer, IDEA algorithm for encryption of mobile agents and RSA key encryption	Using MD5 for message digest and PKI with RSA for digital signatures	Using Java authentication and Authorization service	Using audit functions of java
[25,26]**Focus:** Enhance the traditional non agent-based system. **Issues:** Claimed that agents are interactive, autonomous, extensible, and mobile- allows agents to perform their task with minimum user interaction	A token is send to the receiver who has sign and send it back to the sender to receive the key to decipher the information	Apply cryptographic protocol. The key to decipher the text kept with the information of the sender. -using symmetric keys; AES or Blowfish with key length as variable. -SHA1: to create hashes of the content and secure channel with SSL	PKI to encrypt via RSA algorithm and SHA1 for hash creation	Not discussed	Compared with socket-based system- many weaknesses on that system due to dependent on user availability.
[27]**Focus:** Enhance all e-health organization functionalities using a multi agent system using JADE framework	Not discussed	Vulnerable- using simple firewall, login and password to protect sensitive data In the future proposed of using Elliptic Curve Cryptography	Not discussed	Not discussed	Not discussed
[28]**Focus:** mobile agent system using the Short Message Services(SMS) **Issues:**Malicious mobile agent risk –pilfering of sensitive data, damage to host resources, denial of services and annoyance attacks	Not discussed	Mobile agent generated by SMS – written in specific Mobile Agent Description Language (MADL) – mobile agent generation done separately from mobile agent owner thus will not contain malicious code	Not discussed	Not discussed	Not discussed
[29]**Focus:** Improve existing Virtual Electronic Patient Record (VEPR) system to work on network and distributed medical system **Issues:** To ensure only authorized staff can access the information and data security while moving through network	Using X.509 certificates and Secure Assertion Markup Language (SAML)	Using hash-chains scheme	Creating a digital envelope using public key cryptography signatures, symmetric keys and code decryption.	-Role Based Access Control (RABC)- manage users' role policies - uses Extensible Access Control Markup Language (XAMCL) – ensure interoperability of the system access control	Not discussed

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[30]**Focus:** Provide protections for mobile agent's code and their baggage **Issues:** Existing solutions only detect/prevent attack on agent but no effective solutions for confidentiality of agent's code and baggage	Not discussed	Mobile agent data is encrypted at multiple layers, where only the allowed mobile agent platform can access or look at data Agent's code protection: Every Agent is encrypted with the symmetric key inside PKCS7 SignedAndEnvelopedData	Agent platform restricted to only add data of their own, data alteration is not possible since the data is already encrypted by other mobile agent platform keys	Based on the evaluation of Agent Platform Authorization Polices by PDP, if the result is 'permit' then agent platform gets keys from KDS which can only reveal the data allowed for that particular agent platform which restricts unauthorized access	Not discussed
[31]**Focus:** to protect agent's data using address forward and data backward mechanism which resist colluded truncation attack in free roaming mobile agent and identifies the malicious host.	Not discussed	Using encryption, decryption and Signature Verification Principle. During data collection process the data is signed along with the host's private key, this signature information will be certified	Using the address collection. Secondary agent may check whether the address collection had been damaged or not because the data encrypted using Task Sponsors public key.	Not discussed	Not discussed
[32]**Focus:** Provide a secure path for data protection of free roaming mobile agent.	Mobile agent move to other host according to the trust value and reputation value	The retrieved information is protected using RSA and ECC algorithm	Using secure hash algorithm (SHA)	Mobile agent construct routing table with a Trust Reputation Value (TRV) that is obtained from all neighbor host	Not discussed
[33]**Focus:** proposed a non-interaction mobile agent detecting protocol by combining with onion itinerary technology and identity based.	The agent establish the backward chaining of itinerary constructed by initiator – does not require the use of any online trusted third parties. Using shared key authentication.	Using a non-certificate and a simple symmetric key to encrypt information - can reduce the computation of the system and the complexity of certificate management. Use ID-Based signature to make sure the protocol is secure against existential forgery and repudiation attacks.	-	-	No active involvement of trusted third party The itinerary encrypted without using interactive shared session keys-avoid session keys transmit in public and reduce key management burden. Identity based encryption mechanism improved operation efficiency.
[34]**Focus:** Proposed a security protocol which combines self-decryption, co-operation and obfuscation technique with lesser computational cost.	Formal verification using BAN logic	Mobile agent is fragmented into byte arrays and embedded in controller agent. Fragmentation key is encrypted with AES, and AES key with RSA. Controller agent self-decrypt fragmentation key and reassemble mobile agent from byte arrays and executes.	-	Self-decrypting mobile agent	More efficient than traditional AES encryption because only fragmentation key and not agent is encrypted.