ISSN 2250-3153

Secure Auction Bidding Mobile Environment through Randomized Alphanumeric Cipher Algorithm

Sudhakar Kumar Singh, Hariom Kumar and Rajkumar R

School of Computing Science and Engineering, Vellore Institute of Technology, Vellore

Abstract- Mobile Auction Bidding is a developing mechanism that may widely used by GPRS enabled mobile around the world. Many dependable models existing in internet enabled platform. The proposed Auction Bidding Mobile application is basically based on Japanese auction, Double auction and English auction. Making the business model trustworthy, security is being provided by RAC (Randomized Alphanumeric Cipher) Algorithm.

The developed Mobile application has a strong process direction, in contrast to traditional cryptographic approaches, composed of functional module and the best security analysis, in terms of computational time and effective environment over the network. The infrastructure collects location evidences about the buyer authenticity and the behavior can be used in the future to profile bidders in order to detect frauds.

Index Terms- Security, Auction, Bidding, RAC, Mobile

I. Introduction

Mobile Auction Bidding is message authentication auction hence the Auctioneer as well as the Bidder doesn't need to go anywhere; instead they can take part in the auction or bidding during the day or night. The proposed Mobile Auction Bidding has a certain simple process. The only few pre-conditions are that the Auctioneer or Bidder must register and authenticate before he/she can take part in the bidding process. The system uses GPRS forms authentication which creates a session cookie for any signed in user via message authentication. The most important and frequently used method for evaluating the effectiveness of the proposed system is the span of the session and the cookie remains valid until the user logs out. In general, we can classify Message authentication Security Service as Critical Security (CS) where as CS service provides strong security protection by using Randomized alphanumeric Cipher Algorithm which consists of longer key size, strict security access polices, isolation for protecting data, and so on. When a mobile device requests a security service to the GPRS, the system admission controls the entire resource management model about the availability of system resource. The Proposed system maintained the module in such a way so that the closed bid of those products whose closing date is less than the current date is automatically disabled. The process automatically transfers the control and hides it from the users.

The lastly we considered the "Administration" module. Administrator module has been designed in such a way so that it checks all the security apart placing a bid to submission of product. Once the module in session the administrator can add, edit, modify product categories and assign new auctioneer as well as administrator notify both the Auctioneers and Bidders to complete the transaction without fail.

II. Existing Auction Bidding System

Auction Bidding System exists in the Internet based auctions, which are rapidly diversifying into various products. Most notable auction companies are eBay [http://www.ebay.com] for a wide range of daily use products, CNET [auctions.cnet.com] basically for electronic goods, Priceline [www.priceline.com] for air-line tickets, and E*Trade [www.etrade.com] for financial products. These auctions bidding basically based on following mentioned Auction Types.

1. Chinese auction: It is a combination of a raffle and auction that is typically featured at charity and also known as penny social, tricky try or pick-a-prize according to avoid causing offence.

2. Dutch Auction: It is also known as clock auction, an open auction or an open-outcry descending-price auction, where the auctioneer begins with a high asking price instead of asking lower price, auctions reserved until some participant is willing to accept the auctioneer's price, or a predetermined reserve price which means the seller's minimum acceptable price is reached.

3. Sealed-bid first price and Second price auction: It is very common in the stamp collecting business. It is basically seen in markets of refinancing credit and in foreign exchange, which is more common in today's society due to the internet auction website, eBay.

4. English Auction: It is commonly being seen in real estate auctions and car auctions as well as it is widely used in offline and online environments to sell various resources such as art, collectables, electronic devices, and so on.

5. Double Auction: A double auction admits multiple buyers and multiple sellers concurrently into the market. When potential bidders submit their bids and potential auctioneers simultaneously submit their bid prices to an auctioneer, after placing a bid price an auctioneer chooses some price q that clears the market: all the sellers who asked less than q sell and all buyers who bid more than q buy at this price q.

III. Proposed Auction Bidding System

Proposed auction bidding system uses Randomized Alphanumeric Cipher algorithm and applying XOR operation with auctioneers and bidders message and the technique of Bit-stuffing in specific way. We used private key and the public key which increases the efficiency level of encryption algorithm

.Here one 8-bit public key is randomly selected among several generated Alphanumeric Characters and one 5-bit private key. These may vary in real life environment. Our proposed system is basically based on double auction and English auction. During the implementation of proposed system, we also focused on stabilizing revenues in a recurring auction for perishable resources, where the auctioneers must prevent price collapse that requires controlling as well as the supply of resources and solving the bidder drop problem. This system designed in such a way to identify this problem and also attempts to resolve it and provide better security to the system by introducing Randomized Alphanumeric Cipher algorithm to increase the efficiency and also having a tendency to reducing the starvation problem.

IV. Initial Level Architecture of Auction Bidding

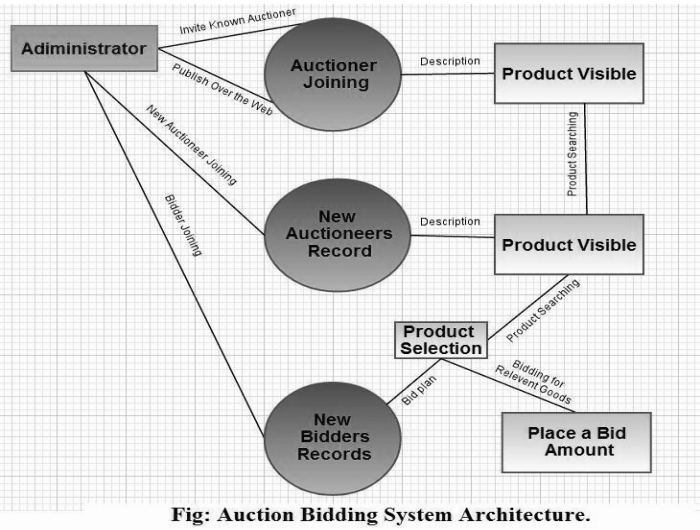

Fig: Auction Bidding System Architecture.

V. Architecture of Bidding Process

Bidding process starts once the auctioneer provided their product details with all mandatory information and verified by the Administrator. After verification of goods, N number of Bidder can take part and during bidding time stamp M number of bidder can also join. Once the session is being expired the process automatically transfers the control to the closed bidding module and hides the expired product details from the bidding log. Once all the verification is being done Administrator announced the winner and notifies both the Auctioneers and Bidders to complete the transaction without fail.

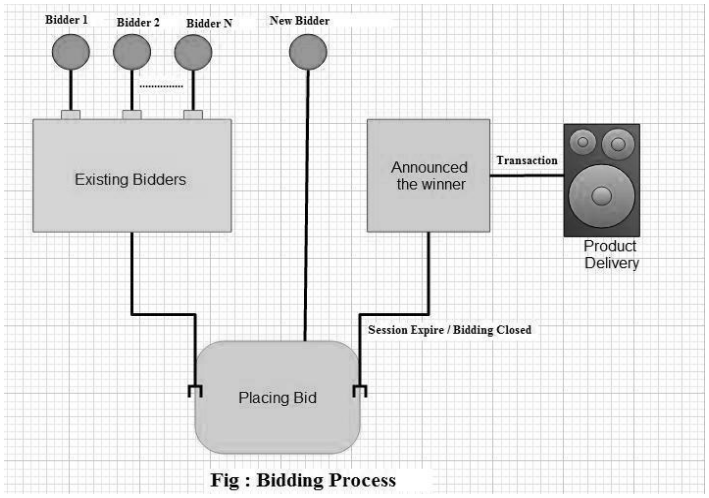

Fig : Bidding Process

VI. Security Consideration for Auction Bidding

During the bidding process our proposed security mechanism will ensure that the police are not sabotaged by an external bidder who is not a part of auction. To avoid unauthorized posting and make reliable system, bid is being done by silently and data is being saved in encrypted form. Encryption and deception is being based on RAC, since we are basically dealing with the mobile auction so that our proposed system will take care of the memory space before saving the encrypted data. This mechanism not only provides incentive compatibility, efficiency, and individual rationality but also minimizes the communication overhead and the expected revenue of allocating the resources. This behavior ensures the reliability and trustworthy of auction bidding system.

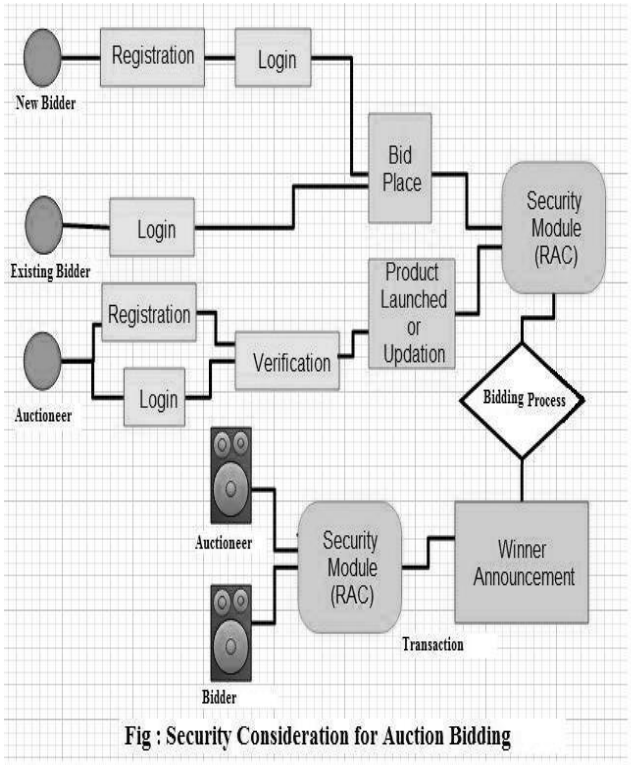

Fig : Security Consideration for Auction Bidding

VII. SECURITY MODULE OF RAC

Encryption Algorithm

1.Generate N number of 8-bit Alphanumeric Characters randomly
2. Randomly select any one among them, denoted as 'A', and 5-bit SECRET KEY assigned as 'B'.
3. Convert 'A' and 'B' in binary format.
4.Compute the quotient of these two Q=A/B.
5. Perform XOR operation with Message 'M' and quotient 'Q', TEXT = M XOR Q.
6. Scanned TEXT and perform the Bit-Stuffing.
7. In this way we get the encrypted message as CIPHERTEXT.

Decryption Algorithm

1. Remove the extra bit from CIPHERTEXT.
2. Perform the XOR operation with 'TEXT' and quotient 'Q'.
3. In this way we get the original message 'M'.

VIII. CONCLUSION

Overall online /offline Auction Bidding plays an important role in the existing commercial environment, But due to lack of information people missed the chance of participating in auction bidding system. Hence our proposed System places an important role to fill the gap via Mobile auction bidding. It also insures that the proposed system will take care of all Security issues by applying RAC and make the model reliable and trustworthy over the mobile environment. As the resultant, our proposed system is one of the useful systems over the mobile devices.

REFERENCES

[1] S.C. Coutinho,University Press (India) Private Limited (2003).The Mathematics of Ciphers ,Number Theory and RSA Cryptography.

[2] Department of Computer science Federal University of Rio de Janeiro Rio de Janerio, Brazil.

[3] Evolution of Cryptography Mohd Zaid Waqiyuddin Mohd Zulkifli, Evolution of Cryptography, 17th January 2007.

[4] Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology, B.Ravi Kumar et al. / International Journal on Computer Science and Engineering (IJCSE).

[5] Sudhakar Kumar Singh - Design and Implementation of Cipher Algorithm using Randomized Alphanumeric Characters - published at: "International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 Edition".

[6] Franklin, M. & Reiter, M. (1995), the design and implementation of a secure auction services, in 'Security and privacy' proceedings. 1995 IEEE Symposium.

[7] D. L. Reiley, "Auctions on the Internet: What's Being Auctioned, and How?"Journal of Industrial Economics, 48(3): 227-252.

[8] T. Sandholm, "Approaches to winner determination in combinatorial auctions", Decision Support System, 28 (1):165 - 176.

[9] Wikipedia, The Free Encyclopedia, from http://en.wikipedia.org/wiki/Auction

[10] Agorics, Inc., "Going, Going, Gone! A Survey of Auction Types", available at

[11] http://www.agorics.com/Library/auctions.html

[12] C.A. Johnson, "Commentary: The boom in online auctions", article by forester research, 2002, available at http://news.com.com/2009-1069-962530.html

AUTHORS

First Author – Sudhakar Kumar Singh, M.Sc (Computer Science), VIT University, Vellore, Email: Sksingh2012@yahoo.com

Second Author – Hariom Kumar, M.Sc (Computer Science), VIT University, Vellore, Email: khariom58@yahoo.com

Third Author – Rajkumar R, Assistant Professor (Senior)-SCSE VIT University, Vellore