Kerberos based Electronic Auction System

Nitish Kumar Singh
School of Computer Engineering KIIT University, BhubaneswarOdisha, India

Yashwant Singh Patel
School of Computer Engineering,KIIT University, Bhubaneswar,Odisha, India

ABSTRACT

An electronic auction (e-auction) system is an auction system in which a process of selling, buying and other services are provided with the help of online software, In the modern era e-auction system is increasing rapidly and because of its popularity the need of quality and security are also increasing. In this paper a 'KBEAUCS' model is proposed which provides user an another way of participating in auction irrespective of the geographic locations and without worrying about security threats.

General Terms

Security

Keywords

KBEAUCS, Kerberos, AS, UID, Credit Card, TGS.

1. INTRODUCTION

Traditional auction systems which were based on some rules for exchange and these rules were used for buying and selling goods or several type of services and then selling the item up to the highest price. But this auctioning system has several type of issues like large number of resources, higher cost, different locations for different type of auctions. To overcome these issues, in recent years e-auction system has widely used in many different formats. There are some popular auction algorithms such as English, Dutch, Vickery auctions and Sealed-bid used over the internet[1].

The popularity of e-auction system is increasing day by day ,due to this popularity the fraud related activities are also increasing[2].

In this paper, a model KBEAUCS is proposed which uses concept of Kerberos. Users who are interested for e-auctioning have to download an application on their mobile, now they are able to participate in e-auction and they will also be unaware from background processes. The basic purpose of this model of e-auction is to increase security and quality of an e-auction system.

2. RELATED WORKS

The first Web browser for the Windows and Macintosh platforms was released at the end of year 1993. The auctions were already in use even before the release of this browser with the help of email discussion lists and text-based newsgroups of Internet[3].

The earliest auctions which opened in May 1995, were Web-based auctions appear to have been Onsale and in September 1995 ,eBay is opened [3].

In 1997 Onsale started to supplement its site of merchant with a service of auction listing similar to which of eBay, later this auction service of person-to-person transferred to Yahoo[3].

In 1998,Onsale declared that it would start to offer fixed-price selling of electronics at prices of wholesale and in 1999 it announced an another online retailer known as merger Egghead[3].

In the year of 2002, due to the fast expansion of the popularity of the e-commerce form, online auctions or e-auctions were aimed to account for 30% of all online e-commerce[4] .

Recently it has seen that e-auctions websites are also used by thieves for the purpose of selling stolen things to unsuspecting buyers[5].

According to the record of police there were above 8000 crimes which involves fraud or deception, stolen goods on e-Bay in the year of 2009[6].

In the scenario of Shill Bidding where there is a provision of putting fake bids which benefits the seller of the product is oftenly used in Online auctions and can also be seen in standard auctions. In the year of 2011, a member of e-Bay became the first individual, who convicted of shill bidding on an auction[7].

To avoid the auction frauds various models were proposed like NetProbe- for the purpose of fraud detection in online auction network[8], Secure auction protocol based on the semantics of BAN-style logic[9], Formal verification to analyze the security characteristics of e-auction protocols[10], Secure auction protocol based on digital signature and encryption technology[11] etc.

But still there is a need of such a system which can provide security and robustness to an e-auction system from different kind of unauthorized activities.

3. THE PROPOSED ELECTRONIC AUCTION SYSTEM

In this section an E-Auction system named KBEAUCS is proposed. This system contains three stages: Pre-registration, Post-registration & Accessing e-auction services. These three stages are described in later section. These three stages are explained one by one.

3.1 Pre-registration stage

The user who wants to use electronic auction system, sends message to authentication server. The message contains UID card number and Credit card number. The authentication server will receive three things, UID card number, Credit card

number & corresponding mobile number, which this message has contained.

Authentication server will send user's mobile number to SIM card issuing company. The SIM card issuing company will send user's detail such as user's name, date of birth, address, father's name, e-mail id etc.

Now authentication server will also send UID card number to UID card issuing authority. UID card issuing authority will send user's details such as user's name, date of birth, address, father's name, e-mail id etc, corresponding to that mobile number which are common to that send by UID card issuing company. Authentication server will also ask to Credit card issuing authority for credit information by sending the user's credit card number. The credit card issuing authority will send user's credit details such as user's previous profile, available credit corresponding to that credit card number. The authentication server will verify user's details provided by UID and SIM card issuing authority and also verify user's credit card information and will check that user is eligible to participate in e-auction or not.

After successful verification, the authentication server will send one session key which is a randomly generated key and one TGS key (which is generated with the help of UID and Credit card number) for Ticket granting server (TGS) to user which are encrypted with symmetric key by the authentication server and this symmetric key is already known to TGS. Now user will request for using services of e-auction system with TGS key. TGS will decrypt the TGS key with its own symmetric key and verify that user is authenticated or not. If user is verified then TGS will send one user-id and password with the address of application server to the corresponding user in ACK.

There may be a scenario where user can change his/her mobile number in that case user has to send a message to authentication server. This message contains UID card number, Credit card number & old number which user has already registered for e-auction. After performing the above procedure, If successful registration is done, then authentication server will send a acknowledgement to user. This will confirm the user about successful updation in his/her mobile number[12].

3.2 Post-registration stage

In this phase user will request for e-auction application from the given application server address by TGS then application server will send an application on his/her mobile phone. After installing successfully, an icon will be displayed. whenever user wants to use the e-auction services, he/she simply double click on that icon, after clicking on icon an interface will appear. User has to enter his/her user id and password and click on login button. After clicking on login button, an encrypted message will be created and send to Application server this message contains user's login details, Application server will decrypt the received message and verified it. If it is successfully verified then application server will send an acknowledgement of confirmation, if it is failed then it will send an acknowledgement according to kind of failure that is occurred in the process of verification.

3.3 Accessing e-auction services stage

After successful completion of post-registration stage user will be directly switched to e-auction application and authorized to use services of e-auction system such as join as buyer, join as seller, profile (for both buyer and seller), categories of different products etc.

4. THE PROPOSED E-AUCTION ALGORITHM

The steps of KBAUCS model are given below:

A. *Pre-registration Stage*

1) User Ui sends his/her UID number Uid and Credit card number CCi in message Mi i.e.

$$Mi = f(Uid, CCi)$$

for $i = 1,2,3,\ldots..$ number of users

2) AS receives message Mi along with MOi mobile number.

3) AS sends message Mi^1 to SIM card issuing company i.e.

$$Mi^1 = f(MOi)$$

4) AS also sends message Mi^2 to UID card issuing authority i.e.

$$Mi^2 = f(Uid)$$

5) AS also sends message Mi^3 to Credit card issuing authority i.e.

$$Mi^3 = f(\mathrm{CC_i})$$

6) AS verifies Ui's validity and has not applied for registration before this.

7) AS will update its database and send ACK which contains session key and TGS key to user Ui.

8) Now user Ui will send the request Ri for e-auction system along with TGS key to TGS.

9) TGS will send the ACK which contains user-id and password to the corresponding user.

B. *Post-registration stage*

1) User Ui will fill the user-id and password and then click on login button.

2) After pressing on the login button it will generate an encrypted message i.e.

$$Mi^{\mathrm{E}} = f(Uid, \text{Password})$$

3) Application server will receive Mi^{E} and send acknowledgement of confirmation to the corresponding user Ui.

C. *Accessing E-auction services stage*

1) User Ui will perform the transaction of given choice.

2) and after completion he/she can logout the session.

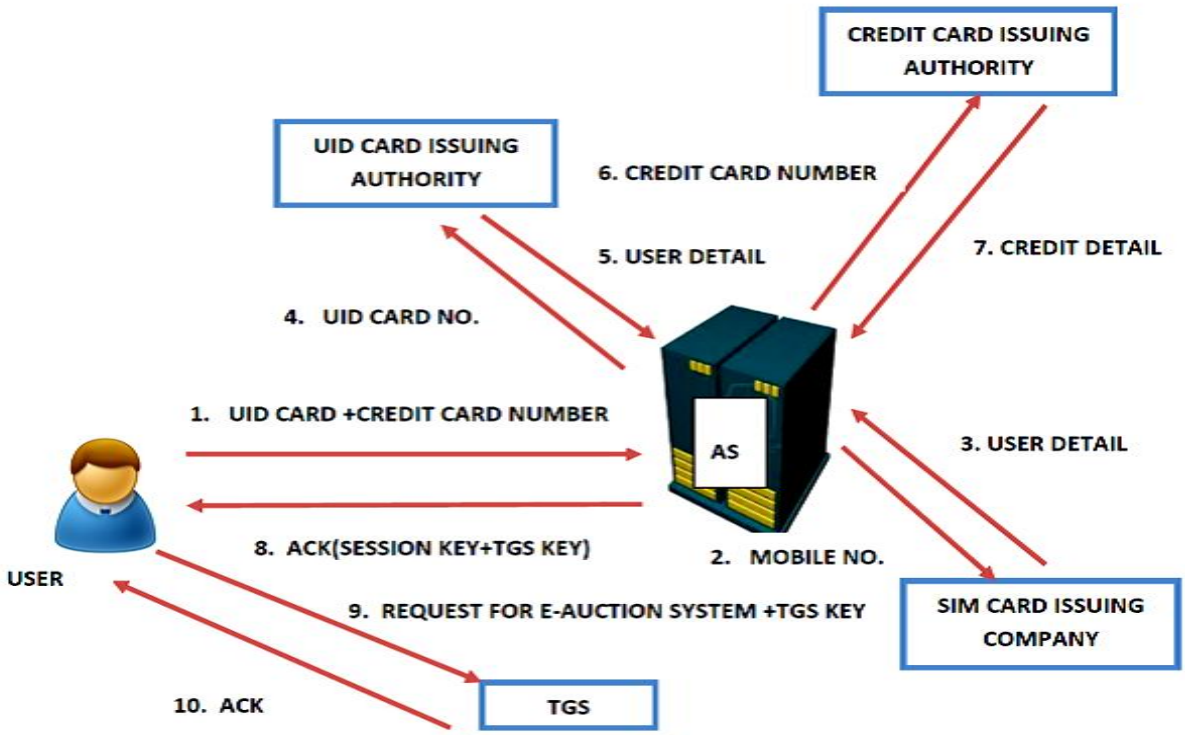

Fig 1: Pre-Registration stage

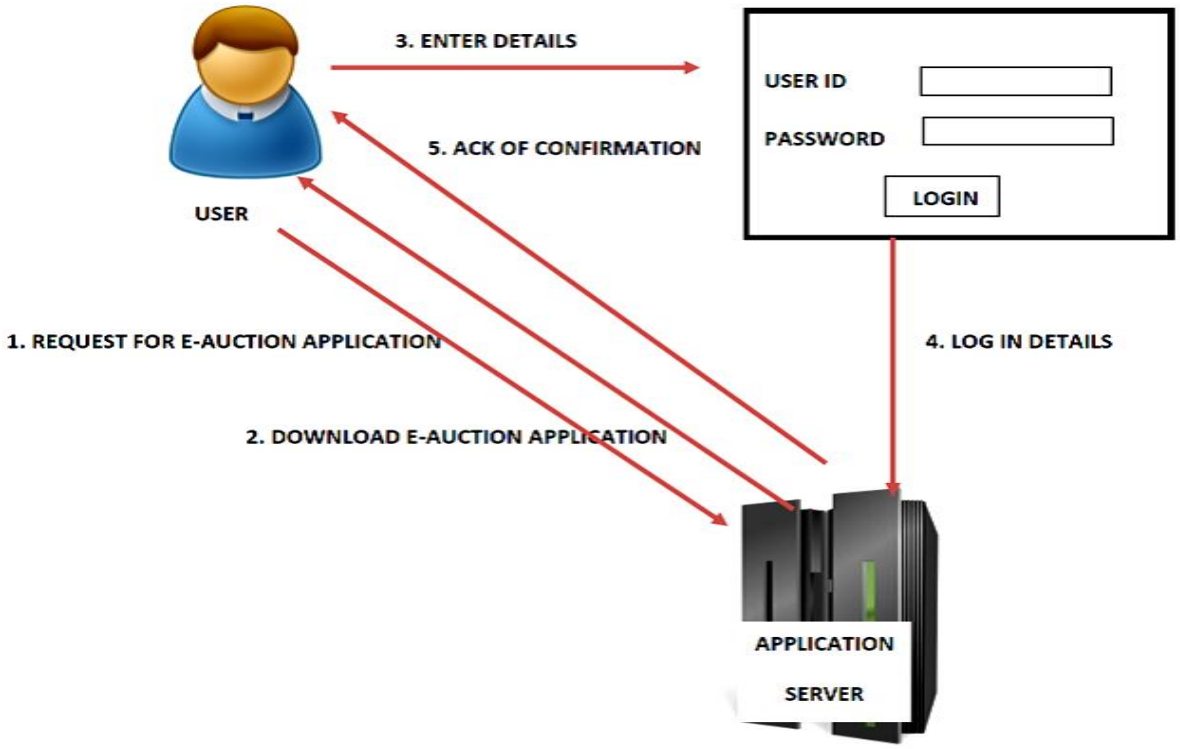

Fig 2: Post-Registration stage

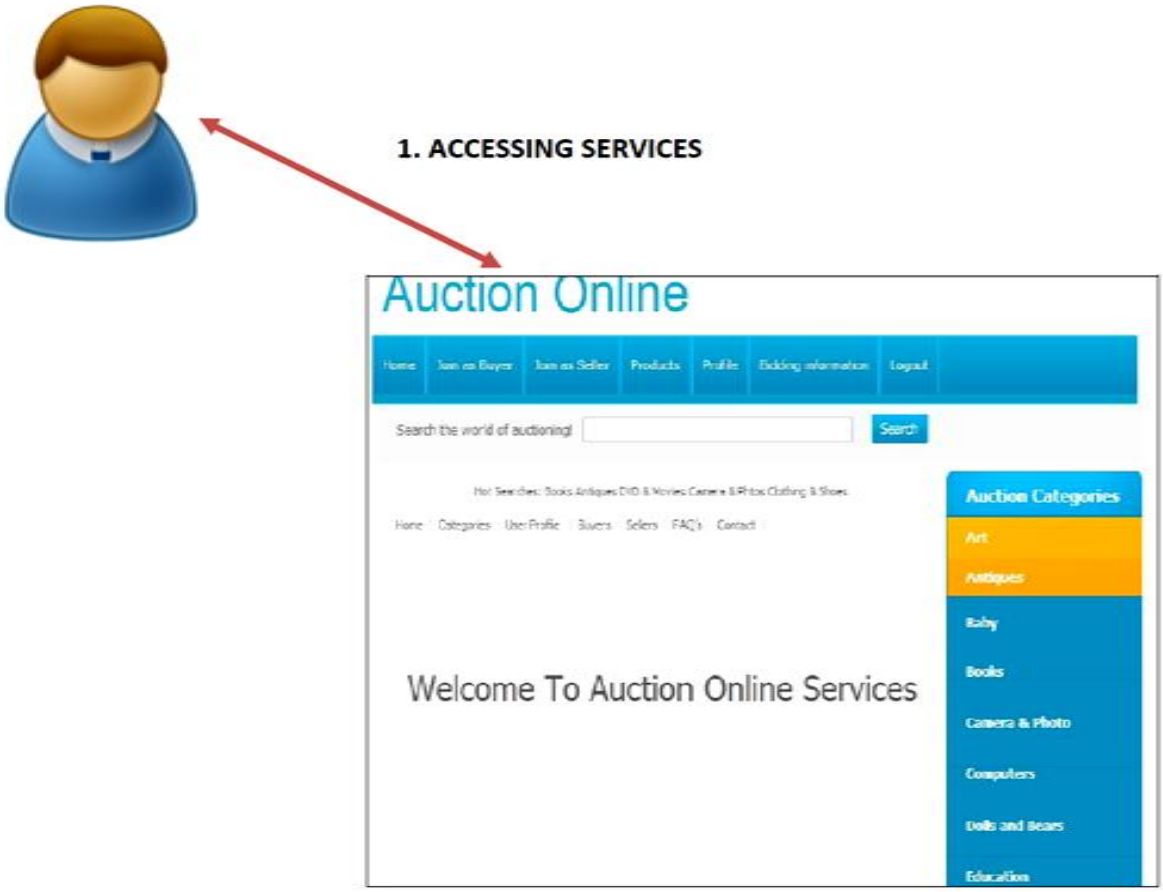

Fig 3: Accessing e-auction services stage

5. CONCLUSION

Kerberos based e-auction system assures a vision for providing security in the future, this system provides a secure channel which is used for providing communication between different entities. Apart from Kerberos's many strengths, it has some weaknesses and some limitations[13].

In this paper a KBEAUCS model is proposed, which can handle all earlier issues occurred in a traditional auction system, KBEAUCS model provides security from unauthorized happenings like selling of stolen things, occurrences of frauds during buying and selling, security threats by attackers and intruders. Purpose of this model is to enhance the level of security during an e-auction process so that user can trust the system and user can easily use the e-auction system without any hesitation. This model is secure, easy to understand and transparent and it can also be used with some other technologies.

6. ACKNOWLEDGMENTS

This work was supported by KIIT University, Bhubaneswar, Odisha. Our thanks to the experts Prof. Amitavo Sen, Prof. Manoj Kumar Mishra, Prof. M.N. Das and Our senior Virendra Kumar Yadav for their valuable suggestions during various discussion sessions they had made.

7. REFERENCES

[1] P. Hemantha Kumar, Gautam Barua (2001), "Design of a Real-Time Auction System" 4th International Conference on Electronic Commerce Research, Dallas, Texas, USA, November 8-11, 2001.

[2] Miriam R. Albert (2008), "E-buyer beware: Why online auction fraud should be regulated", Article first published online: 28 Jun 2008 , American Business Law Journal, Volume 39,Issue 4, June 2002, pp 575-644.

[3] David Lucking-Reiley (2003) ,"Auctions on the Internet: What's Being Auctioned, and How?",Article first published online: 27 Mar 2003, The Journal of Industrial Economics, Volume 48, Issue 3, September 2000, pp 227-252.

[4] Vakrat, Y., Seidmann, A. (2000), "Implications of the bidders' arrival process on the design of online auctions", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences,2000.

[5] San Jose Mercury News (2002-06-11) "Stolen-Property Purchases Leave Ebay Buyers Burned" (http://www.highbeam.com/doc/1G1- 120375160.html).

[6] The Sunday Times (2009-04-11) "Ebay: Brisk Bidding in stolen goods".

[7] BBC News (2010-07-05) "Man fined over fake eBay auctions"(http://news.bbc.co.uk/newsbeat/hi/technology/newsid_10500000/newsid_10508900/10508913.stm).

[8] Shashank Pandit, Duen Horng Chau, Samuel Wang, Christos Faloutsos Carnegie Mellon University , (2007), "NetProbe: A Fast and Scalable System for Fraud Detection in Online Auction Networks". In proceedings of the 16th international conference on World wide web, New York, NY, USA, ACM Press.

[9] Subramanian, S. Dept. of Comput. & Inf. Sci., Ohio State Univ., Columbus, OH, USA, (Oct 1998) "Design and verification of a secure electronic auction protocol", In proceedings of Seventeenth IEEE Symposium on Reliable Distributed Systems,1998,pp 204-210.

[10] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech Universite Grenoble 1, CNRS, Verimag, FRANCE, (2013) "Formal Verification of e-Auction protocols". In proceedings of Second International Conference on Principles of Security and Trust,, Lecture Notes in Computer Science Volume 7796, 2013, pp 247-266.

[11] Qinghua Xiao, Coll. of Comput. Sci., Zhejiang Univ., Hangzhou, China, Lingdi Ping, (11/2004) ,"A general secure electronic auction protocol", In proceeding of: Systems, Man and Cybernetics, 2004 IEEE International Conference on, Volume: 1,pp 398-402.

[12] Virendra Kumar Yadav, Saumya Batham, Amit Kumar Mallik,(2012) "Kerberos based Electronic Voting System", ICNICT - Number 2 , IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies, 2012 by IJCA Journal.

[13] Steven M. Bellovin, Michael Merritt – AT&T Bell Laboratories, (1991) ,"Limitations of the Kerberos Authentication System".

[14] Shanthi Potla, "Online Auctioning", A Thesis Presented to the Faculty of San Diego State University in the Summer of 2011.