IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Object-Oriented Modelling Of Kerberos Based Authentication Process In E-Banking Transaction

M. Das Nath[1*], S. Karforma[2]

[1]Dept. Of Commerce (IT), St. Xavier's College (Autonomous), Kolkata, India
[2] Department of Computer Science, The University of Burdwan, Bardhaman, West Bengal, India

[*]Corresponding Author: mausumi.dasnath@gmail.com, Tel.: +91-9830659302

Available online at: www.ijcseonline.org

Abstract— The exponential growth and the success rate of different electronic application areas like E-Services, E-Governance, E-Payment, E-Banking, E-Shopping etc is enormously dependant on security, authenticity and integrity of the most confidential information which is sent across the network by the sender. With the increasing menace of several cyber threats, the sender has to feel safe in sending across their identity details over the communication medium. On the other hand, the receiver must receive the same, without any loss or tampering of information as there are several intruders or eavesdroppers waiting to steal the financial data/information. The security parameters cannot be compromised at any cost. Hence, to combat the pilferage of data, different types of authentication protocols and mechanisms have been in use. For example, the banking sector often uses a two-factor authentication, e-commerce merchants go for different layers of authentication and so on. This paper focuses on the use of the most popular authentication protocol, Kerberos, which could be applied for logging in for e-banking system, in order to achieve the highest level of security. Furthermore, we have tried an attempt to use object-oriented modeling to show the working of the authentication with the help of Kerberos and IDEA encryption algorithm as an added level of protection.

Keywords— *Authentication, Object-oriented modeling, Kerberos protocol, IDEA, E-Banking*

I. Introduction

Due to the proliferation of digitized services in different sectors like E-Governance, E-Payment, E-Banking, E-Shopping, security, integrity and authenticity of the sensitive information, sent over the communication network is at risk. Hence, to maintain the network security parameters there is an ardent need of certain authentication protocols. This will eventually prohibit, tampering of confidential data or stealing away the confidential data by unauthorized people. Thus, to combat this growing menace, authentication is necessary. Furthermore, to bring about this endorsement, there should be a security measure to find the authenticity of the user(who is either a customer / bank employee) using the e-banking system. The customer should feel safe and secured while transmitting their data in an open network environment. Before confiding their credentials and financial data, the genuineness of the customer is to be confirmed. Once the customer's identity is verified, he/she can access the products or services provided by the banking system at ease and in a timely manner. The major task of authentication procedure is to find out the validity of the actual person/device requesting for the access of data over the communication channel. The process involves a series of sequential steps required for completing the authenticating phase. Usually, an authentication protocol engages two or more parties and that whoever is involved in the protocol must be aware of the rules before any communication progresses. The most widely used network authentication protocol-Kerberos, can be used in an open or distributed environment. Due to its robustness [3], we can apply in real-life scenario and overcome the hurdles of various network security problems. It is mainly suited for client-server applications where a secret-key cryptography is applied to protect the information. In this paper, we have added the IDEA(International Data Encryption Standard) encryption algorithm [1,13], which will provide an extra layer of protection. Thus, it will maintain the security features in those unsecured environments by protecting the confidential data from unpredictable attacks and Man-in-the Middle Attacks[1]. Hence, it can be very well applied for any e-banking transaction.

Architectural Framework of our Proposed System

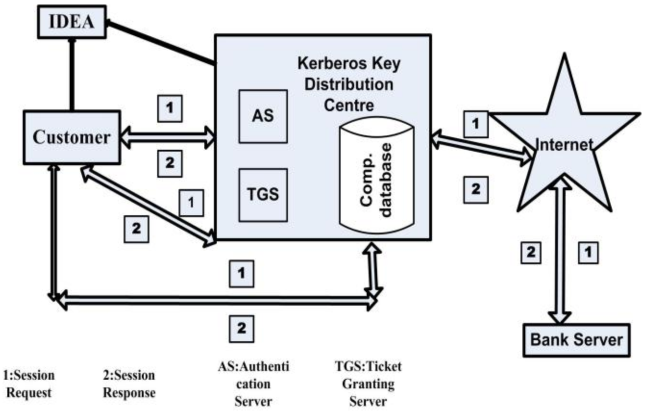

Figure 1: **Diagram of our proposed model**

The above diagram depicts that a customer/client first sends his password to prove his identity. Thereafter, the information is validated from the database at the bank server as well as from the Key Distribution Centre, wherein, the client's details and the password in encrypted form are stored. After successful validation, the customer then sends a request for a session key. This session key is used to encrypt messages between the two parties after which it will expire. The client will decrypt the message to retrieve the session key. Later, the client requests for a ticket from the Ticket Granting Server(TGS) which is server specific. The TGS will issue a response, only after verifying all the details. So, with the ticket to the server and the authenticator, the client will now have access rights to the server he wishes to and gain access to the e-banking system. During the entire process, the encryption and decryption would be taken care of by IDEA (bit block cipher) encryption algorithm, so as to make it highly secured. It operates on 64-bit plaintext blocks. Three different algebraic operations - XOR, Addition modulo 2^{16} and Multiplication modulo 2^{16} are used which operate on 16-bit sub-blocks. As the key length of IDEA is twice as long as DES, it would require $2^{128}(10^{38})$ encryptions to recover a key. In other words, it might take 10^{13} years time.

The presentation of the paper is organized as follows. Section II focusses on the literature review and section III details the working methodology. Discussions are given in Section IV. Section V illustrates the future directions and concluding remarks and finally, section VI presents the references.

II. Related Work

The review is focused on providing information associated with kerberos technology used for authentication for services in banks. As online banking has popularised, secure communication over an unsecured network has become a very crucial and challenging task. Hence, several researchers have illustrated that the implementation of IDEA cryptographic algorithm can highly improve the characteristics of security over an insecure channel.

J.T. Kohl [3] proposed a technique where each user and the network server had a password known to itself, and to the Kerberos database, the database server used it for authentication purpose. But, A. Foz and S. D. Gribble[4] used a proxied implementation of Kerberos, called Charon, to use it for indirect confirmation and secure communication with handheld devices. To overcome the hurdles of weak passwords, the widely used Kerberos authentication protocol has been modified by E. Eman, M. Kouth, H. Kelash and O. S. Faragallah [5] by generating a secret-key for hashing and encryption. Triple-DES technique were used, where password guessing were prevented. Furthermore, a Triple password mechanism have been proposed by G. Dua, N. Gautam, D. Sharma and A. Arora [6] to prevent replay and password attacks. But, E. Eman. M. Kouth, H. M. Kelash and O. S. Farag Allah [7] introduced minor variations to the Kerberos database .They introduced that the secret key will not depend on the user password and thus guessing passwords will be quite difficult. Again J. T Kohl, B.C. Neuman and Y. Theodore [8] in the Kerberos Authentication Service, removed few problems of Kerberos version 4 and proposed solutions in version 5 which was later accepted by other organizations too.

S. Patil and V. Bhusari [9] illustrated that IDEA algorithm with few modications, can reduce the limitations of weak keys too. On the other hand, S. F. Shazmeen and S. Prasad[10] proposed that combining DES, AES with IDEA algorithm secures data transmission from the attackers effectively. Moreover, S. Artheeswari and Dr. R.M. Chandrasekaran [11] portrayed that the short messaging service (sms) could also be made secured in the mobile banking scenario by using IDEA symmetric cryptographic algorithm. And, P. Bhadauriya, F. Suthar and S. Chaudhary [12], presented that IDEA maintains the security features very well with cloud data too.

III. Methodology

The present study finds a model suitable to fill the functional scarcity of the real life E-Banking transactions using Kerberos and IDEA. Kerberos being a strong authentication protocol can be used in the e-banking domain. In the present scenario, the account holder discloses his/her personal identity to the banks in an insecured networking environment. Kerberos can issue a one-time login session key which is time dependant. Once the session key expires, the authenticate customer cannot carry out any further transaction. This prevents from intrusions and from Man-In-the-Middle Attacks . So there is a minimal chance of entry of a third party. Thus, our proposed Kerberos based authentication not only is a secured and trusted communication, it yields in higher reliability during transactions. To further strengthen the system cryptographically , IDEA encryption algorithm might be used with the Kerberos protocol.

In this paper, we have used object-oriented modeling to illustrate the working scenario of an E-Banking transaction. The Unified Modeling Language (UML) is an Object Oriented system analysis and design paradigm which offers generic prototype design technology developed by Grady Booch, James Rumbaugh, Ivar Jacobson in the Rational Software Corporation. This enables us to understand the complex real-life situation in a much simpler way. UML [14] can be used very efficiently to design the model of E-Banking system. With the other traditional methods of design, object-oriented design has become the most accepted one as it helps us to specify, construct and visualize the model more clearly. UML consists of a number of graphical elements that may be combined to form a diagram. The purpose of the diagram is to give a complete detailing of a system which is referred to as a model. UML model describes what a system is supposed to do. It doesn't tell how to implement the system. It includes nine diagrams namely, Class diagram, Object diagram, Use Case diagram, Sequence diagram, Collaboration diagram, Statechart diagram, Activity diagram, Component diagram, and Deployment diagram . Here, we have chosen the Class diagram[14,15] to explain and design our proposed system

Identification of Objects
The objects that are required to design for the proposed system for authentication in e-banking are as follows:
Customer: An account holder of the bank whose credentials are to be authenticated by the Kerberos authenticator.

Kerberos Key Distribution Centre (Kerberos_KDC): Acts as an authenticator for communication between the client and the server. It generates session key in encrypted form, issues ticket to be used for specific server and authenticates to communicate with the server for a service.

Bank Server: Authorizes and authenticates the customer for further transactions in the network.
IDEA: The process of encryption and decryption is taken care of by this algorithm.

Class Diagram
A class diagram gives an overview of the system by describing its classes and the static relationships between them. The following diagram shows four classes: IDEA, Customer, Kerberos Key Distribution Centre(Kerberos_KDC) and the Bank Server. Here, the base class is IDEA, where two methods IDEA_Encrypt() and IDEA_Decrypt() are inherited by the two derived classes-Customer and Kerberos_KDC.

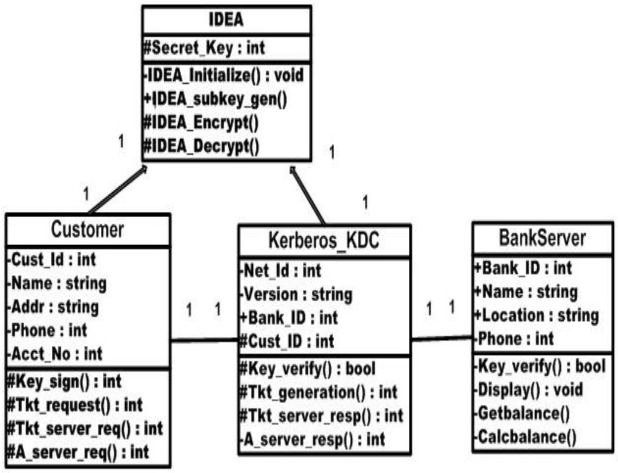

Figure 2: Class Diagram with IDEA as a base class

The customer will input his credentials and it is going to be checked from the database where the details of all the customers are stored. If any mismatch is found, then the client is not validated. After successful validation, the customer can proceed with all the six Kerberos authentication steps to carry out further hassle-free banking transactions. The corresponding attributes and the associated methods are detailed below.Customer(Cust_Id, Name, Addr, Phone , Acct_No), BankServer(Bank_ID,Name,Location,Phone),Kerberos_KDC(Net_Id,Version, Bank_ID, Cust_ID), IDEA(Secret_key).

Customer:
Key_sign() : To login as a valid customer.
Tkt_request(): The client or the customer would request for a Ticket-Granting Service (TGS) from Kerberos.
Tkt_server_req() : To use a particular server, the customer would request a ticket for that server from the TGS.
A_server_req() : The client or the customer will create an authenticator containing his/her name, network address , a timestamp, encrypted with the session key for him/her and the server which the TGS generated. The request will consist of the ticket received from the Kerberos(already in encrypted form including the server's secret key) and the encrypted authenticator.

Kerberos_KDC:
Key_Verify() : To verify the details of a valid customer.
Tkt_generation() : The client or the customer would receive the encrypted secret key for TGS from Kerberos.
Tkt_server_resp() : To use a particular server, the customer would receive an encrypted ticket for that server from the TGS.
A_server_resp() : The server decrypts and checks the ticket and the authenticator along with the client's address and

timestamp. The server would send a response consisting of the timestamp and the encrypted session key.

BankServer:
Key_verify() : Verify and validate the customer information.
Getbalance() :Retrieve account balance .
Calcbalance() : Calculate balance of the account after any financial transaction.
Display() : Displays the balance and the customer details.

IDEA:

IDEA_Initialize()

```
Step1: 64 bit data is inputted.
Step2: It is divided into 16 bit blocks- B1, B2, B3, B4
```

IDEA_subkey_gen()

```
Step1:128-bit key is divided into eight 16-bit subkeys. [Six subkeys are for Round 1 and first two for Round 2].
Step2: Then the key is rotated 25 bits to the left and again divided into eight subkeys. [The first four are used in Round 2 and the last four are used in Round 3].
Step3: The key is rotated again 25 bits to the left for the next eight subkeys.
The process continues till the end of the algorithm.
```

IDEA_Encrypt()

```
Round 1 to 8:
   Step 1: Multiply B1 and the first subkey.
   Step 2: Add B2 and the second subkey.
   Step 3: Add B3 and the third subkey.
   Step 4: Multiply B4 and the fourth subkey.
   Step 5: XOR the output of Steps 1 and 3.
   Step 6: XOR the output of Steps 2 and 4
   Step 7: Multiply the output of Step 5 and the fifth
           subkey.
   Step 8:Add the output of Steps 6 and 7.
   Step9: Multiply the output of Steps 8 with the sixth
           subkey.
   Step10:Add the output of Steps 7 and 9.
   Step11:XOR the output of Steps 1 and 9.
   Step12:XOR the output of Steps 3 and 9.
   Step13:XOR the output of Steps 2 and 10.
   Step14:XOR the output of Steps 4 and 10.
```

The output of the round is the four sub-blocks that are the outputs of steps 11 to 14. Swapping the two inner blocks except for the eighth round and that would be the input to the next round.

Round 9 gives the final output transformation stated below:

```
   Step1: Multiply B1 and the first subkey.
   Step2:Add B2 and the second subkey.
   Step3:Add B3 and the third subkey.
   Step4:Multiply B4 and the fourth subkey.
```

Thus , the four sub-blocks are reattached to produce the encrypted text.

IDEA_Decrypt()

Here, decryption is same as that of encryption, except that each of the 52 16-bit subkey used for decryption is the inverse of the subkeys used during encryption. Moreover, the subkeys are reversed during decryption in order to reverse the encryption process. The all-zero subkey is considered as 2^{16} =-1 for multiplication modulo 2^{16}+1.

IV. DISCUSSIONS

From previous research work , it has been noted that IDEA being a very strong cryptographic algorithm, will give better results in terms of time and reliability. When implemented with a robust network authentication protocol, it will definitely reduce data theft in a highly insecured network. In addition, this would build a trust in the customer's mind that his/her financial credentials won't be tampered or stolen.

V. CONCLUSIONS AND FUTURE SCOPE

From the above discussion, it is to be seen that our proposed model using the network protocol- Kerberos, combined with IDEA algorithm would be beneficial in nature, both for the Bank as well as the Customer during electronic banking transactions as it is very difficult to crack an IDEA encryption with 128 bit keys. The idea of 8 rounds in IDEA is immune to different attacks during data transmission[1,2,10].It maintains privacy, integrity as well as confidentiality in those unsecured environments by protecting it from several erratic attacks. In this paper, we have used object-oriented modelling to explain the working of the system. Furthermore, we have made an attempt to identity the various objects involved, their tasks and how they interact and associate with other objects in the proposed system.

As an extension of this work, we can apply for M-banking too, and test it for large amount of data.

REFERENCES

[1] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C", Wiley Computer Publishing, John Wiley & Sons,Inc.,pp. 266-271,470-475,2007.

[2]W. Stallings, "Cryptography and Network Security", Pearson,5th Edition, 2011.

[3] J.T. Kohl,. "The use of encryption in Kerberos for network authentication." In Conference on the Theory and Application of Cryptology, pp. 35-43. Springer, New York, NY, 1989.

[4] A.Fox, and S D. Gribble. "Security on the move: indirect authentication using Kerberos." In Proceedings of the 2nd Annual International Conference on Mobile Computing and Networking, Berkeley, USA, ACM pp.155-164, 1996.

[5] E.El-Emam,M. Koutb, H.M. Kelash, and O.S. Faragallah. "An Authentication Protocol Based on Kerberos 5." IJ Network Security ,Vol.12,No. 3,pp.159-170, 2011.

[6] G. Dua, N. Gautam, D. Sharma, and A. Arora. "Replay attack prevention in Kerberos authentication protocol using triple password", International Journal of Computer Networks & Communications (IJCNC) , Vol.5, No.2, March 2013.

[7] E.El-Emam, M.Koutb, H.Kelash, and O. Farag Allah. "An optimized Kerberos authentication protocol", International Conference on Computer Engineering & Systems 2009, ICCES 2009,Cairo, Egypt, pp. 508-513,IEEE, 2009.

[8] J.T Kohl, B. Clifford Neuman and Y. Theodore. "The evolution of the Kerberos authentication service", 1994.

[9] S.Patil & V. Bhusari," An enhancement in international data encryption algorithm for increasing security", Intl. J. of Application or Innovation in Engineering & Management, Vol.3.No.8, pp. 64-70,2014.

[10]S. F. Shazmeen,S. Prasad,"A Practical Approach for Secure Internet Banking based on Cryptography", International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012, ISSN 2250-3153.

[11]S. Artheeswari, Dr. RM. Chandrasekaran, "INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) FOR DATA SECURITY IN CLOUD", "International Journal of Technology and Engineering System" (IJTES),Vol 8. No.1, Pp. 06- 11,Jan- Mar 2016, ISSN: 0976-1345.

[12] P.Bhadauriya, F. Suthar & S. Chaudhary, "A Novel Technique for Secure Communication in Cryptography". IJARCCE, pp.328-331, 2017.

[13] S. Basu, "INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION", International Journal Of Global Research in Computer Science, July 2011.

[14] J. R. Rumbaugh , M. R. Blaha, W. Premerlani, F. Eddy,W. Lorensen,"Object-Oriented Modeling And Design", Prentice Hall of India Private Limited, India,pp.16-17,1998.

[15] R. Mall, "Fundamentals Of Software Engineering" Fourth Edition, Prentice Hall of India Private Limited, India pp.276-334, 2014.

Authors Profile

Mausumi Das Nath is working as an Assistant Professor in the Department of Commerce(IT) at St. Xavier's College (Autonomous), Kolkata. She completed MCA, PGDIT (Symbiosis, Pune) and M. Tech (IT).She has 18 years of teaching experience and 5 years of research experience. Her research interests include Network Security, Image Processing and Data Mining.

Dr. Sunil Karforma is currently working as an Associate Professor in the Department of Computer Science, The University of Burdwan , India. He is serving as an editorial member and reviewer of several international reputed journals. Dr. Sunil Karforma is the member of many international affiliations. He has successfully completed his Administrative responsibilities and has authored many research articles/books related to Artificial Intelligence Network Security Database Security DRM.