Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.120 – 127

RESEARCH ARTICLE

Analysis and Improvement in Kerberos 5

Romendrapal Singh Rathore
M.Tech. Scholar, Department of Computer Science & Engineering,
Mewar University, Gangrar, Chitorgarh
rjsingh.r@gmail.com

B. L. Pal[1], Shiv Kumar[2]
Assistant Professor, Department of Computer Science & Engineering
Mewar University, Gangrar, Chitorgarh
[1] contact2bl@rediffmail.com, [2] shivkumar004@gmail.com

Abstract — *Kerberos is an authentication protocol in which client and server can mutually authenticate to each other across an insecure network connection, to ensure privacy and data integrity. We take a close look at Kerberos's authentication technique using Secret key cryptography.. This thesis presents a Study and analyzes of existing framework model and policies for authentication services. The criteria expose the strengths and weaknesses of existing system. We have proposed a design and framework for authentication using Kerberos 5. The proposed modification in Kerberos 5 will be more Protectable from replay attack., eavesdropping, password guessing attack, differential brute force attack and more useful in Cross-realm authentication.*
This design and framework can be used for those who need to choose an infrastructure, knowing the Kerberos broadly. The characteristics presented here are proposed to enhance the security and efficiency of transactions in Kerberos 5 over a network.

Keywords: Authentication, AES-256, SHA-512, BBS&MM, Cross-Realm Authentication, Active Attack

I. INTRODUCTION

Kerberos provides a means of verifying the identities of principals, (e.g., a workstation user or a network server) on an unprotected network. Its purpose is to allow users and services to authenticate themselves to each other means, it allows server and user to demonstrate their identity mutually. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the statement that packets roving along the network can be read, modified, and inserted. Kerberos relies heavily on authentication technique involving conventional cryptography, i.e., shared secret key. The basic concept is simple: if a secret is known by only two people, then person can confirm the identity of the other by verifying that the other person knows the secret.

It requires additional servers -Authentication Server, and Ticket-Granting Server. When client is authenticated, it gets TGT (Ticket-Granting Ticket) from Authentication Server. With TGT, client can get Ticket for specific server from a Ticket-Granting Server. With Ticket, client can login application server. We can see the authentication process in figure 1 . The advantage of Kerberos system is that a user does not need to register in each server, and each server does not need to have each user's username and password in their storage. Clients can log on to a server in two steps. First, they get

authenticated at the Authentication server (AS), and get a Ticket- Granting Ticket (TGT). The client presents the TGT to the Ticket-Granting Server (TGS) and gets a real Ticket for a specific server [1].

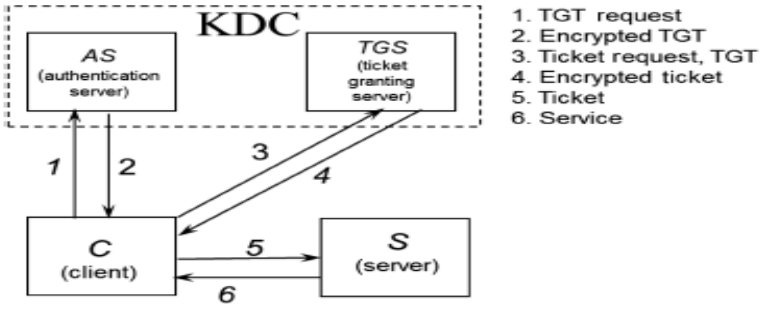

Figure 1: Kerberos System [2]

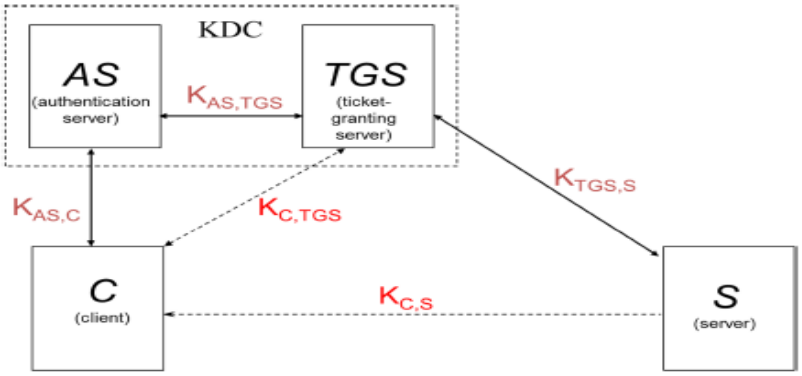

Figure 2: Keys in Kerberos [2]

With this ticket, clients can log onto an application server. It is shown in Figure 1. Using the Tickets, Kerberos never sends a password over the network, so the password is protected against eavesdropping or replay attacks. A ticket contains the authentication information of the ticket holder, and is encrypted with the key of the final recipient. so a client holding a ticket has no knowledge of the ticket's content nor can they modify it. As it is encrypted, it can be safely sent across the networks. The types of keys are described in Figure 2. The shared keys, KAS, TGS, KAS, C , KTGS , S are predefined during the registration process, and KC,TGS , KC,S are dynamically generated during authentication.[2]

II. LITERATURE REVIEW

In this section, the existing solution techniques for Kerberos authentication protocol are analyzed. Kerberos security considerations and basic operation of Kerberos in communication networks are explained in detail. Additionally, solution techniques of Kerberos for various networks are elaborated. The merits and weaknesses of Kerberos and its solution techniques are critically analyzed.

The NNCC scheme can be best used for on-line e-commerce transactions. NNCC is more practical than other Kerberos-based systems as it can work under the current card payment system with only minor changes. NNCC inherits most of the advantages of Kerberos. to make NNCC usable in an off-line environment, a mobile phone application with an Internet connection should be developed[2] .Extensible Pre-Authentication in Kerberos (EPAK), describes a Kerberos extension that enables many authentication methods to be loosely coupled with Kerberos, without further modification to Kerberos. EPAK extends just the initial authentication phase to allow the security infrastructure built up around Kerberos to remain unchanged. Unlike existing Kerberos extensions, EPAK enables the integration of many authentication methods without further modification to Kerberos implementations. EPAK benefits both Kerberos and the systems it integrates with Kerberos. additional authentication protocols can be incorporated into Kerberos using EPAK to test its extensibility and guide further enhancements[3]. In Security issues and attacks in distributed system , different security aspect like information security , physical security , technical security of networks are discussed. All these securities should be

properly implemented in distributed environment. Security of distributed system is more complex than stand alone system security and needed some more effort[4]. A collaborative trust enhanced security model for distributed system in which a node either local or remote is trustworthy this approach enhances the performance of complete system by sharing the authentication workload among all other nodes. To accomplish this goal, It was devised an agent based system with various functionalities as monitoring the servers, balancing the load of service providers and service request in case of unavailability of servers. It shall deploy CTES model with web services on large scale [5]. Distributed Authentication in Kerberos Using Public Key Cryptography address through the integration of public key cryptography with traditional Kerberos authentication. Public key based systems rely on Certificate Authorities as trusted intermediaries when authenticating clients and servers [6]. The computational requirements of public key cryptography are much higher than those of secret key cryptography, and the substitution of public key encryption algorithms for secret key algorithms impacts performance. This system uses closed, class-switching queuing models to demonstrate the quantitative performance differences between PKCROSS and PKTAPP—two proposals for public-key-enabling Kerberos. It has shown that, while PKTAPP is more efficient for authenticating to a single server, PKCROSS outperforms the simpler protocol if there are two or more remote servers per remote realm[7]. SHA-512 is faster than SHA-256 on 64-bit machines is that has 37.5% less rounds per byte (80 rounds operating on 128 byte blocks) compared to SHA-256 (64 rounds operating on 64 byte blocks), where the operations use 64-bit integer arithmetic [8].Biometric security is concerned with the assurance of confidentiality, integrity, and availability of information in all forms, in this work focused on biometric authentication along with all security assurance. Authentication of a person is an important task in many areas of day-to-day life including electronic commerce, system security and access control. It presents Kerberos a client\server authentication protocol which can perform a secure communication over unsecured environments [9]. In Existing Kerberos, Triple-DES in CBC mode as an encryption algorithm, SHA-256 as a hashing algorithm, and Blum Blum Shub as a random number generator algorithm. The introduced modifications to the KDC database will enhance the performance of the protocol since the principle's long-term secret-key will be independent of the user password. Thus, this modified Kerberos version is no longer vulnerable to password guessing attacks. it tested implementation on a small LAN and are looking forward to extend implementation to cover cross-realm operations[10]. HMAC cannot be used if the number of receivers are more , because a symmetric key is supposed to be shared only by two parties one sender and one receiver, receiver is unable to know that the message was prepared and sent by the sender, and not by one of the other receivers[11]. Kerberos can use a variety of cipher algorithms to protect data des-cbc-crc, des-cbc-md4, des-cbc-md5, des3-cbc-sha1, arc-four-hmac, aes128-cts-hmac-sha1-96, camellia128-cts-cmac etc [12].

III. EXISTING (SYSTEM) KERBEROS 5

The principal's secret- key is independent of the user password. It conquer the problem of password guessing attacks which is the main drawback of the Kerberos protocol. Kerberos Distribution Center saves a profile for every request in its realm to generate the principal’s secret-key by hashing the profile, and encrypting the output digest. the lifetime of the secret-key is controlled using the system clock. Triple-Des is used for encryption, SHA-256 for hashing, and Blum Blum Shub for random number generation [10].

Limitations

- Existing(System) Kerberos 5 requires extending implementation in cross-realm operations.
- Triple DES is highly secure but also has the drawback of requiring 168 bits for the key which can be slightly difficult to have in practical situations.
- Blum Blum Shub generator has disadvantage that it is computationally intensive. It takes n2 steps to generate one random bit of the bit-stream.
- SHA-256 is slower, less performer or requires more cost for implementation.

IV. ANALYSIS & FINDINGS

A. Findings

We have found in our analysis that if we use AES-256 in CBC mode as encryption algorithm then it will be more supportable in cross realm mode and protectable from Active attacks. Similarly if we use SHA-512 algorithm as message digest algorithm it will enhance the system performance, confidentiality, and Integrity of system. BBS and MM will help us to build a PRNG that is not only secure and efficient but also fast, and will reduce replay attack[22][8][13].

B. Feasibility Study

- **Operational Feasibility**: In this system there is only training of interaction with user interface. Since the users are computer literate it would not to be difficult to settle in to new system.

- **Technical Feasibility**: The development of the application is feasible. The clients in this setup where Microsoft Windows 7 machines and the local KDC may Windows Server 2008 R2 machines and the remote KDC was a Linux server running KDC on it and the application server was also a Windows Server 2008 R2 machines.

V. PROPOSED MODIFICATIONS IN KERBEROS 5

A. Purpose

To Study and analyze existing framework, model, policies for authentication services. And propose and design a framework for authentication using Kerberos

B Architecture

The network principal may be a client or a server. Every principal in the network is registered in the KDC database by the principal ID. Then the KDC maps this ID to the proper profile where the profile is named with the principal's ID that belongs to that profile. In order to generate the principal's secret key, we apply a SHA-512 hashing algorithm to the principal's profile and then encrypt the output digest with AES-256. We use BBS&MM for token (Random number) generation from Ticket Granting Server and Application server. The Principal Secret Key creation process can be seen in figure 3

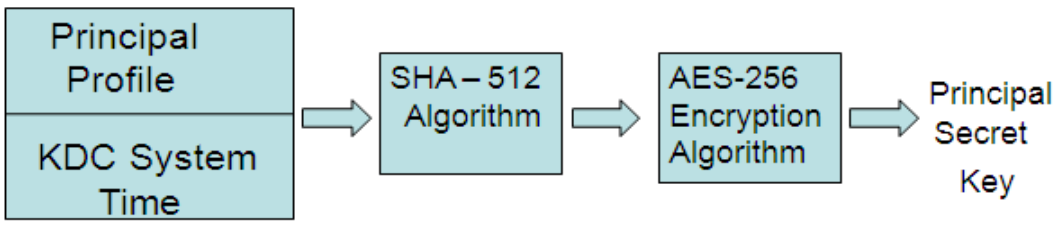

Figure 3: Secret key generation block diagram

C . Authentication Steps

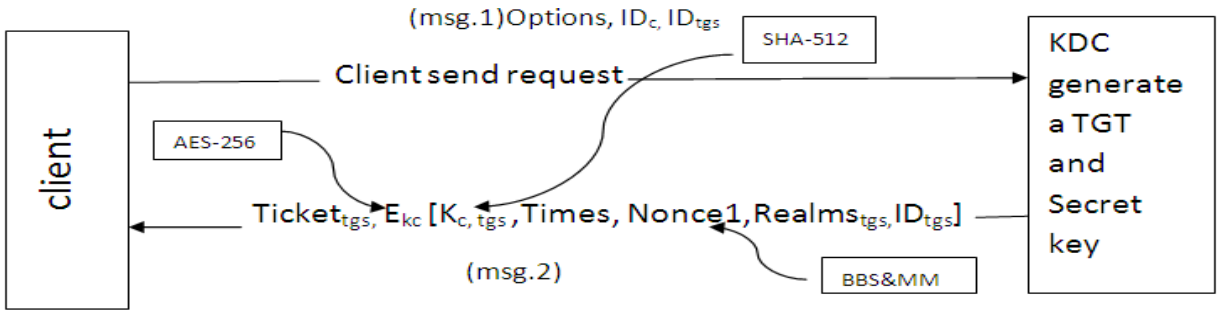

Figure 4: Client request/Reply with KDC

The figure 4 show that initial request is made by the client to the KDC server. The first encryption happens at this point. The KDC however at this point only provides the ticket granting service, for this SHA-512 hashing algorithm will run on principal's profile like on client's password and generate a message digest of this .Then encrypt of this output digest by using AES-256 encryption algorithm. it will be a principal secret key .Now the ticket TGT and secret key will be send to the client. Here the elements used are describes as follows –

ID_C	ID of client	K_c	Key of client(session key)
Options	Setting of flags for returning ticket	Times	Certain time setting in return ticket
ID_{tgs}	ID of Ticket Granting Server	Nonce	Random Number
$Ticket_{tgs}$	Ticket for TGS	$Realms_{tgs}$	Nodes managed by KDC
E_{kc}	Encryption of session key		

Table 1 : The elements of the Proposed Modification in kerberos 5

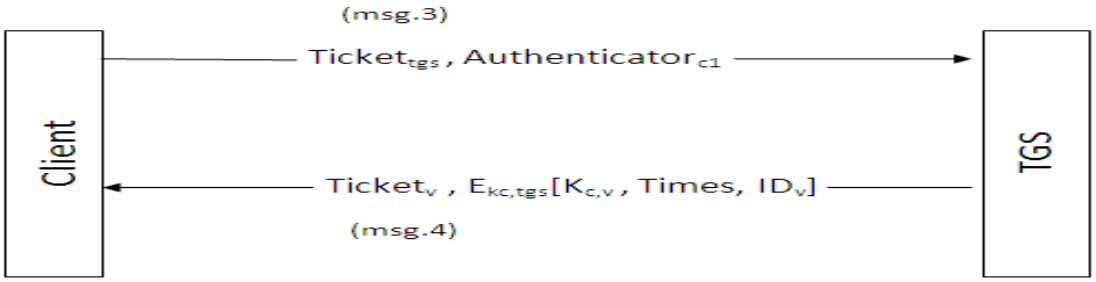

Figure 5: Client Request/Reply with TGS

Figure 5 shows that , Client then deciphers the ticket it got from the KDC and then uses the session ticket provided by the KDC to request for further validation from the Ticket Granting server. Now there is one more deciphering at the Servers end to authenticate the ticket provided by the client.

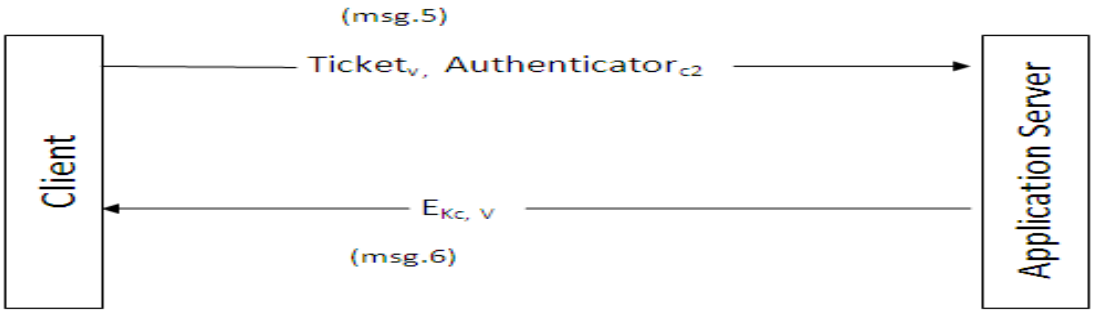

Figure 6: Client Request/Reply with Application Server

Application server will repeat the above process and finally issue the ticket to client for accessing the services from server. It has been shown in figure 6.

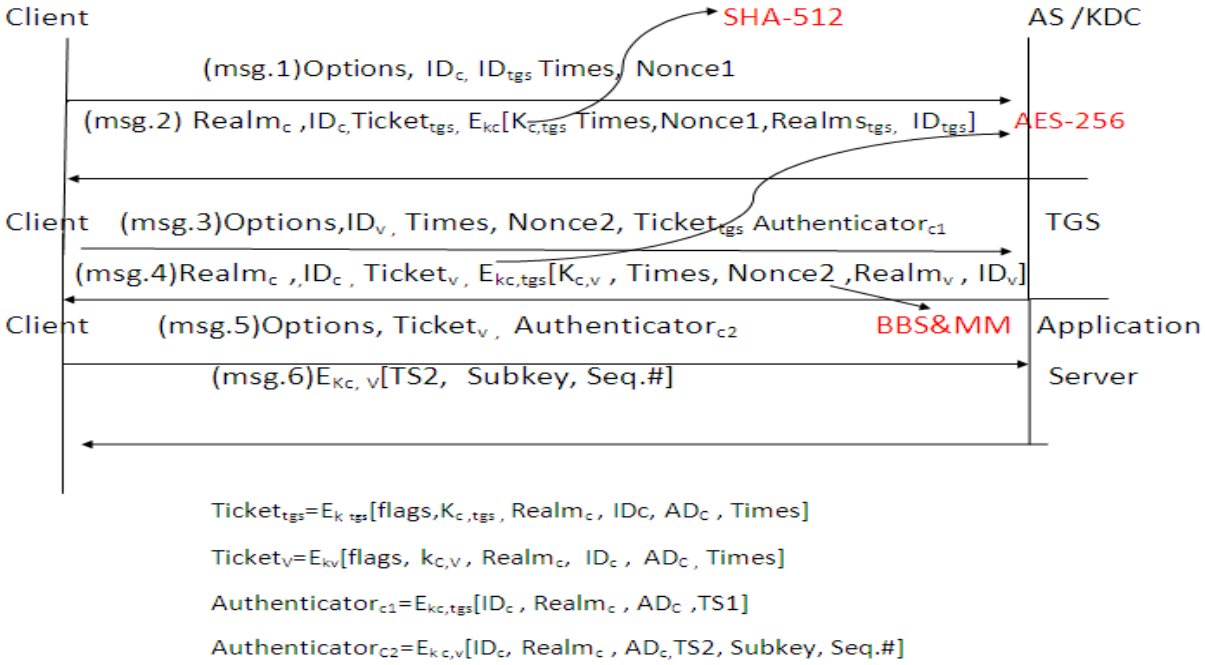

Figure 7: Authentication dialogue for the proposed modification in Kerberos 5[10].

The total number of authentications is recorded on each side for a transaction. In each step at the server side (Authentication server, Ticket Granting Server) a token number (Random Number) will be generated by using BBS&MM algorithm. SHA-512 Algorithm use the client's password to encrypt this random number for creating the message digest (Session key) .This random number will always be different in request/reply process between client and server So the output digest will also be different. So any possibility of replay attack and password guessing attack would never be happened because message digest create at intruder' system will not matched at server side. The total request /reply process in our system has shown in figure 7.So This system will be feasible and provide better results at the time of implementation while AES-256 is used for encryption, SHA-256 for hashing, and BBS&MM for random number generation.

VI. CONCLUSIONS

AES is faster in software and works efficiently in hardware. The NSA has approved the 128-bit AES for use up to SECRET level and 192-bit and 256-bit AES for use up to TOP SECRET level. AES is replacement for 3DES AES has theoretical advantage over 3DES for speed and efficiency in implementation Also, AES has been carefully tested for

many security applications. SHA-512 is safe and resistant to brute force attacks. It is broadly used for digital signature generation. These functions are used to verify the integrity of a message and protect against eavesdroppers SHA-512 algorithm delivers a 50% performance improvement over similar implementations of SHA-256. The storage costs for implementing SHA-512 can be reduced by adding a small amount of one-off computation to compute the SHA-512 constants which will be useful for constrained implementation environment. and with these features it makes the message digest more complex and difficult to break. Montgomery Multiplication has a number of attractive functions in Cryptography and building a Quadratic Residue Cipher, based on BBS that uses Montgomery Multiplication (MM), when BBS and MM put together, they can help us to build a PRNG that is secure, efficient and fast.

This proposed system achieves Confidentiality, Integrity and Authentication is achieved through encryption of the message and protect against eavesdroppers. It is secure and scalable to support a large number of clients and servers. This system would be able to work across two realms so cross realm implementation operations may be done. Availability of the service can be improved by providing fast, reliable and efficient service. This system will not be supportable with Public key cryptography

FUTURE WORK

In future we propose a system that will combine the characteristics of RSA, SHA- 512 or BBS&MM . This will be useful for implementation in Asymmetric environment. As there is already a request to design the next version of Kerberos with AES included, this analysis would be of great help to compare the performance of the variants.

ACKNOWLEDGEMENT

I would like to thank my Guide Mr. B.L. Pal and Co- Guide Mr. Shiv Kumar for their guidance and support during writing of this thesis, especially for commenting and suggesting improvements of the text and diagrams. I would also like to thank them for encouraging me to write the text and for solving related formal issues.

REFERENCES

[1] Anush krishnamurthy , " performance impact of encryption Algorithms on Kerberos network Authentication protocol 2000," M.S. Thesis , Oklahoma State University , May 2006.

[2] Jung Eun Kim, Yoohwan Kim ,"A Secure Credit Card Transaction Method Based on Kerberos" Journal of Computing Science and Engineering ,Vol. 5 , No. 1, pp. 51-70, March 2011.

[3] Phillip L. Hellewell, Timothy W. van der Horst, and Kent E. Seamons," Extensible Pre-Authentication in Kerberos ," Internet Security Research Lab , Brigham Young University Provo, UT, USA.

[4] Manoj Kumar, Nikhil Agrawal**, "**Analysis of Different Security Issues and Attacks in Distributed System A-Review," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013**.**

[5] Aruna Kumari, Shakti Mishra, D.S. Kushwaha, "A New Collaborative Trust Enhanced Security Model Distributed System*,"* International Journal of Computer Applications (0975 - 8887) , Volume 1 – No. 26, 2010.

[6] Marvin A. Sirbu, John Chung-I Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography*,"* Carnegie Mellon University, Pittsburgh, Pennsylvania 15213.

[7] Alan H. Harbitter, Daniel A. Menascé, "Performance of Public-Key-Enabled Kerberos Authentication in Large Networks*,"* PEC Solutions, Inc., George Mason University**.**

[8] Shay Gueron 1,2, Simon Johnson 3, Jesse Walker4, " SHA-512/256*,"* 1 Department of Mathematics, University of Haifa, Israel , 2 Mobility Group, Intel Corporation, Israel Development Center, Haifa, Israel, 3 Intel Architecture Group, Intel Corporation, USA, 4 Security Research Lab, Intel Labs, Intel Corporation, USA.

[9] Shashidhar M S, Suresha D ,"Implementation of Secure Biometric Authentication Using Kerberos Protocol," International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 3 March 2013.

[10] Eman El-Emam, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah, "An Authentication Protocol Based on Kerberos 5," International Journal of Network Security, Vol.12, No.3, pp.159 -170, May 2011

[11] R. Kogila,"An Enhanced Authentication Scheme Using Kerberos with Hash-Based Message Authentication Code (HMAC)," IJCSMC, Vol. 2, Issue. 7, pp.350 – 355 , July 2013.

[12] "Encryption types," *http://web.mit.edu/kerberos/krb5-1.13/doc/admin/enctypes.html, October 15, 2014.*

[13] M.G.Parker, A.H.Kemp, and S.J.Shepherd, "Fast blum-blum-shub sequence generation using montgomery multiplication," Vol. 147, pp. 252–254 , 2000.
[14] Baskett, F., et al., "Open, Closed and Mixed Networks of Queues with Different classes for customers," J.ACM, 22(2), 1975.
[15] Bruell, S.C, and G.Balbo,"Computational Algorithms for Closed QueuingNetworks," The Computer Science Library, ed. P.J.Denning, New York; Elsevier North Holland, Inc., 1980.
[16] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," Journal of computing, Volume 2, Issue 3, March 2010.
[17] "Kerberos : The network Authentication Protocol, " http://web.mit.edu/kerberos .
[18] Ms. Jasmin Bhambure, Ms. Dhanashri Chavan, Ms. Pallavi Band, Mrs.Lakshmi Madhuri, "Secure Authentication Protocol in Client– Server Application using Visual Cryptography," IJARCSSE Volume 4, Issue 2, February 2014.
[19] Sanket Bhat, Saumitra Damle, Priyanka Chaudhari, Abhijeet Saraogi , " KERBEROS: An Authentication Protocol," IJARCSMS, Volume 2, Issue 2, February 2014.
[20] Dr. Salem Sherif Elfard , "Justification of Montgomery Modular Reduction," Advanced Computing: An International Journal (ACIJ), Vol.3, No.6, November 2012.
[21] Simar Preet Singh, and Raman Maini, "Comparison of data encryption algorithms," International Journal of Computer Science and Communication, Vol. 2, No. 1, , pp. 125-127, January-June 2011.
[22] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma , " Analysis and Comparison between AES and DES Cryptographic Algorithm," International Journal of Engineering and Innovative Technology, Volume 2, Issue 6, December 2012

