ISSN:2229-6093

Prof.T Venkat Narayana Rao et al, Int. J. Comp. Tech. Appl., Vol 2 (4), 816-822

An Implementation of BLOWFISH Encryption Algorithm using KERBEROS Authentication Mechanism

Ch Panchamukesh
Assistant Professor
Department of Computer Science and Engineering
HITAM, Hyderabad, India
mukesh_1229@gmail.com

Prof.T.Venkat Narayana Rao
Professor and Head
Department of Computer Science and Engineering
HITAM , Hyderabad, India
tvnrbobby@yahoo.com

A.Vijay Kumar
Assistant Professor
Department of Computer Science and Engineering
HITAM, Hyderabad, India
vijaykanna@live.com

Abstract

The sensitive information stored on computers and transmitted over the Internet need to ensure information security and safety measures. Without our knowledge, the Intruders sneak into the systems, misuse it and even create back doors to our computer systems. Thus, there must not be any compromise in securing our resources. Hence, Cryptography is mainly used to ensure secrecy. Access Control Policy is used for securing the resources as initial state, which determines the potential threats, the solutions and the ways of implementation of the security. Various security solutions to block the unauthenticated users starts from a series mechanism from Firewalls to Kerberos, most of them need a strong cryptographic base. Cryptography provide solutions for four different security areas confidentiality, authentication, integrity and control of interaction between different parties involved in data exchange ultimately which tend to the security of information. Among which Kerberos authentication promises most secured and unbreakable. It works on the basis of granting tickets for each session and resource access. This paper includes a mechanism that implements the Blowfish algorithm with a 64 bit length key with an improved security assurance.

***Keywords*: Kerberos, System Policy, Threats, Security, Public Key Infrastructure, Attack**.

1. Introduction

In this era of E-commerce tools being used for rapid growth in business. The world has globally connected with internetworking, where in sharing of data has become more important. Internet is used in different ways to increase in the growth of the business. But the big question is that our data which is transmitting in the network is secured against unauthorized access or not. The networks have become more task critical and more vulnerable to malicious intents [7], [1]. Every critical data about anybody connected to the net is available for trade or free distribution.

The first situation of threat starts to a web server with the infamous is denial of Service attacks. It is a potential threat where most of the threats come from unauthenticated users, which can cause loss of millions of dollars. So if the security system can block all of these users, almost all the potential problems can be resolved, and it can be also detected by various software tools [6].

But the desire for information is still there with the people. Hackers and virus carriers are becoming more refined and law enforcement needs to learn a more about computer technology and the ways to punish such people. Though data encryption is a good means of security, they take a long time for their operations to be performed which reduces the speed of data transfer and the capabilities of the network. The Kerberos authentication method is almost unbreakable and totally depends upon Encryption and Public key Infrastructure (PKI). This paper implements KERBEROS authentication mechanism to provide the security.

1.1 Types of Network Threats

Basically there are three types of risk:

- Bugs or misconfiguration problems in the Web server that allow unauthorized remote users to:
  - Steal confidential documents.
  - To modify the system configuration.
  - Gain information about the Web server's host machine that will allow them to break into the system.
  - Making the machine temporarily unusable by launching denial-of-service attacks.
- Browser-side risks:

Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely creates an annoyance and misuse of personal information.

- Eavesdroppers can manage from any point on the pathway between browser and server including:
  - The network on the browser's side of the connection.
  - The network on the server's side of the connection (which includes intranets).
  - The end-user's Internet service provider (ISP).

- The server's ISP.
- Either ISP's regional access provider.

Secured browsing plays an important role in protecting the confidential information against network eavesdropping. So, without system security on the browser and server sides, confidential documents are susceptible to interception.

1.2 Methods to attack

Depending on security parameters and the access control policy Attack methods are categorized into:

- Message/session blocking
- Theft of assets
- Eavesdropping
- Sniffers
- Masquerading
- Message forwarding / printing
- Password determination /forging
- Spoofing

To get control of our system or getting access to our files an attacker uses any one of the above ways.

1.3 Security Mechanisms

An organization which uses Internet for their daily transactions and communications should define their own access control policy for appropriate user authentication and authorization as depicted in figure 1.

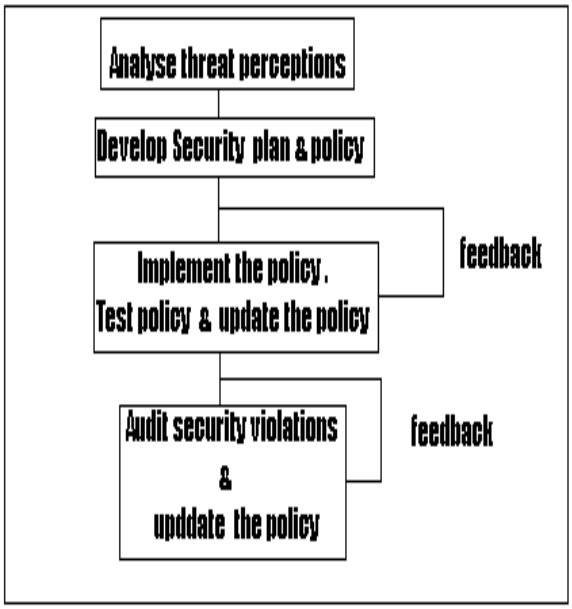

Figure 1: Security Policy Implementation

The organization should always update their policies in accordance with the novel emerging technologies and their loopholes, and also considering their customer sophistication, satisfaction and speed of communication.

1.4 Solutions to attacks

Various techniques are used to solve the attacks on the system and to implement the security policies. These techniques differ from one another by the way of implementation, place of implementation and the application to the layers of the TCP/IP network. They are:

- Authentication
- Firewalls and auditing
- Data Encryption
- Kerberos Authentication

2. Network Security Framework Overview

2.1 Authentication

Authentication of a user in a network can be done either by digital signatures or by digital certificates, which offers the rights and privileges to access our resources for that particular user. This process can also be implemented using firewall systems. Authentication of a user and the document which is sent with Digital Signature can be done by using a public key architecture. A Hash algorithm like **md5RSA** is used to generate a message digest which is concatenated with the information about the signer, a time stamp etc [11][1]. Sender's private key is encrypted with the message digest which produces a encrypted data which is called as "Digital Signature" and which is sent along with the original document to the recipient as shown in figure 2 and figure 3.

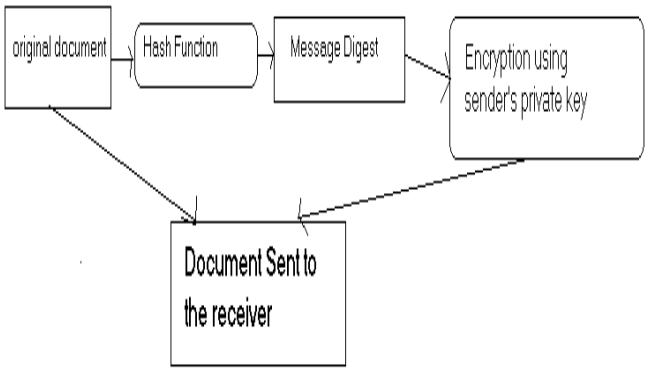

Figure 2: Digital Signature Creation

On the other side of the sender, the receiver accepts the sender's public key and uses it to decrypt the signature. The same Hash algorithm which was used at the sender's side will be used at the receiver's end to compute the original message from the message digest and will be verified with the decrypted signature and if obtained results are same, then the user authenticates the server otherwise erroneous message is declared and the receiver would not accept the document.

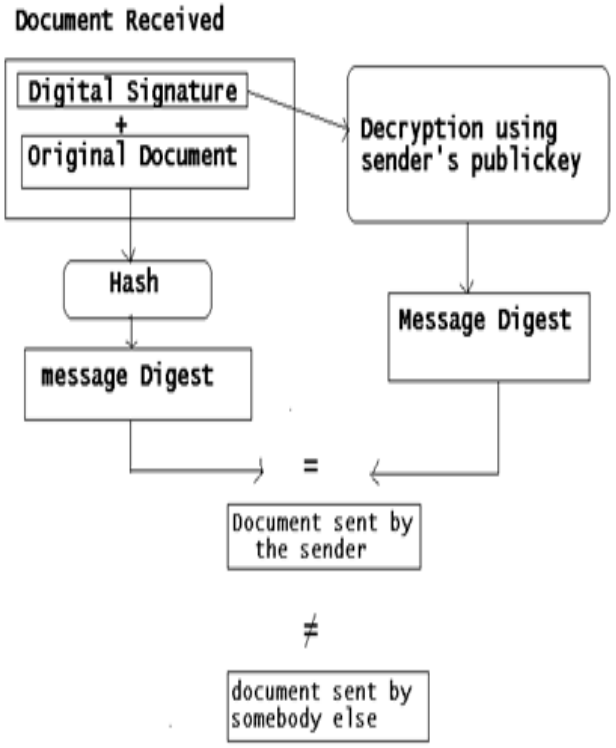

Figure 3: Digital Signature validation

2.2 Firewalls and Auditing

A firewall is a system or groups of systems which enforce the access control policy between two networks. Firewall blocks all the unauthenticated logins to our system. They provide a single choke point where security and audit can be imposed. By auditing the entry log files, we can determine all the security violations and various countermeasures can be taken. They provide the important auditing tool and provide the logging summary about the amount of traffic passed through them. But the Firewall and auditing cannot protect our system against data driven attacks.

2.3 Data Encryption

Science which deals with codes and passwords is known as Cryptography as shown in figure 4. Cryptology is divided into cryptography and cryptanalysis [1],[3],[14]. The Cryptography protects the data, and cryptanalysis hack the protected data. Cryptography provides solutions for four different security areas - confidentiality, authentication, integrity and control of interaction between different parties. The cryptographic encryption algorithms play key role in providing security to the information in the systems.

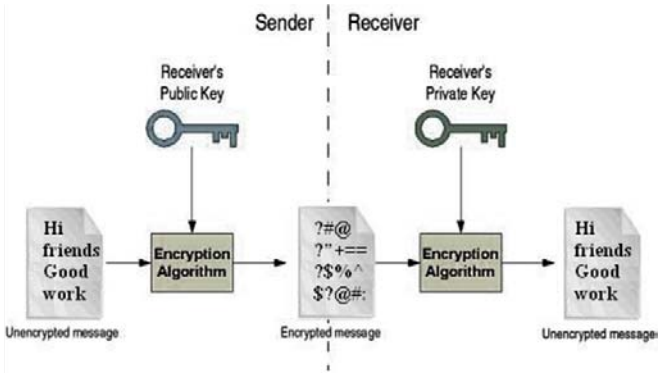

Figure 4: Basic of Cryptology

Cryptographic Algorithms plays a major role in implementation of encrypting the data. As the complexity of algorithm is high the risk of breaking the original plaintext from that of cipher text is less. Greater complexity means greater security. The existing algorithms are categorized into any one of the following types.

- Public Key Algorithms
- Secret Key Algorithms

2.4. Guarding with Kerberos

Kerberos – the God of underworld in Greek mythology. And is the name of the three-headed dog that guards the castle of Hades Kerberos authentication is the network security protocol developed by the students of MIT and is implemented through Windows 2000 and is available as open source or in supported commercial software which is considered as unbreakable[2],[13],[10]. It authenticates a login without ever sending the password on the network.

2.5 Kerberos Tickets

Kerberos works on the theory of granting and verifying "tickets" between clients and servers. Here each ticket provides access to certain resources in the network. When the user uses his username to log in to the network, it is transmitted to the server and the password gets encrypted using a 56 / 128 bit RC4 algorithm in this process a hash function of this password is generated and is transmitted. This is a one-way product of a function and cannot be restored to its original value.

The hashed version of the password is also stored in its active directory. Here, the user is authenticated only after the server verifies that the two hash functions matches. The actual process of authentication is complicated and involves sessions and tickets granted then verified. This is done by a service running in the server called Kerberos Distribution Centre (KDC) [8],[11].

Domain Name
User Name
Ticket Flags
Secret /Session Key
Start Time
End Time
IP Address
Authentication Data

Figure 5: Structure of Ticket Granting Ticket

3. Design and Implementation of the System

Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits (32-448 bits in steps of 8 bits; default 128 bits) [4],[12]. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes.

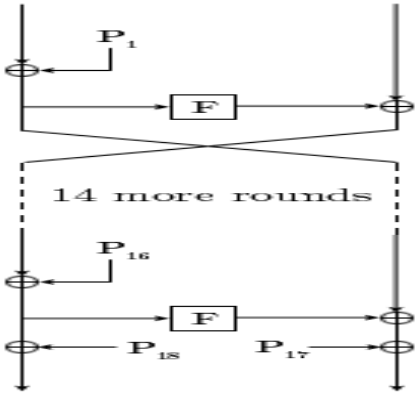

Figure 6: Rounds of Blowfish

The Fig [6] shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries as depicted in figure 6.

The Figure 7 shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes [2]. The outputs are added modulo 232 and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the cipher text block, then using the P-entries in reverse order as explained in figure 6, 7, 8 and 9.

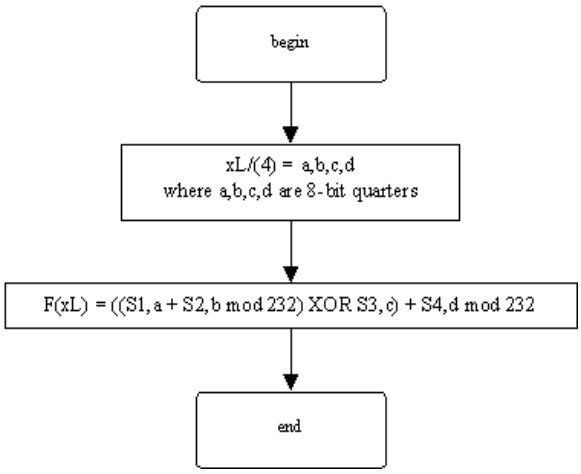

Figure 7: Representation of F-Function

The implementation of the blowfish is represented as in the below flowchart.

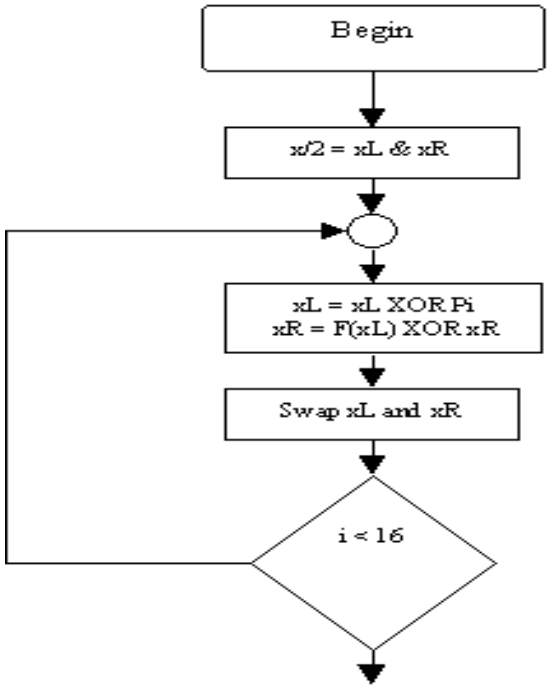

Figure 8: Blowfish Algorithm

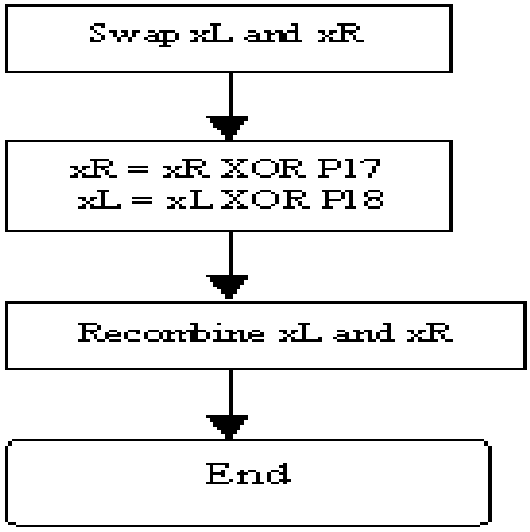

Figure 9: Blowfish Algorithm

The process of implementing the security process using Kerberos has the following four stages:

- Authentication Exchange.
- Ticket-granting service Exchange.
- Client/Server exchange.
- Secure Communication.

3.1 Authentication Exchange

Whenever client asks the authentication server for a ticket to the ticket-granting server (TGS), the authentication server searches its database for the client address and then generates the session key (SK1) which is encrypted by the Kerberos using the client's secret key. The session key which is generated is used amid the client and the TGS. TGS's secret key (known only to the authentication server and the TGS) is used by the authentication server to create and send the user a ticket-granting ticket (TGT) as explained in figure 10.

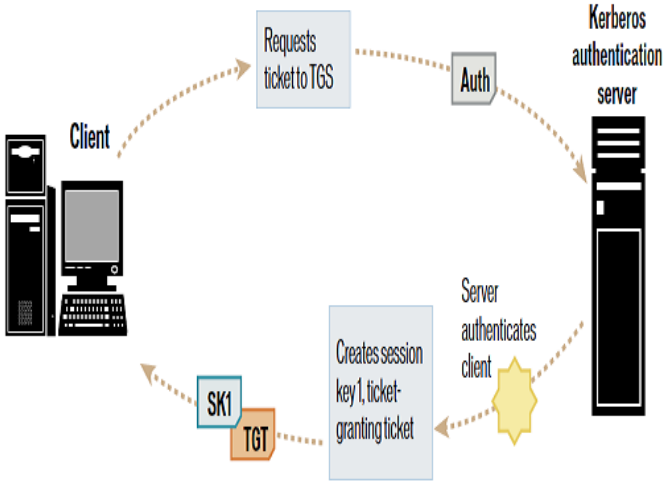

Figure 10: Authentication Exchange

3.2 Ticket-Granting Service Exchange

The message received by the client is decrypted to recover the session key to create an authenticator containing the user's name, IP address and a time stamp. This authenticator is sent by the client along with the TGT, to the TGS to access the target server as depicted in figure 11 and 12. The TGS decrypts the TGT, and then uses the SK1 inside the TGT to decrypt the authenticator. The information in the authenticator, the ticket, the client's network address and the time stamp is verified by the TGS to precede the request to access the target server. A new session key (SK2) is created by the TGS for the client and target server to use. SK2 is encrypted using SK1 and sent to the client along with a new ticket containing the client's name, network address, a time stamp and an expiration time for the ticket. All are encrypted with the target server's secret key and the name of the server.

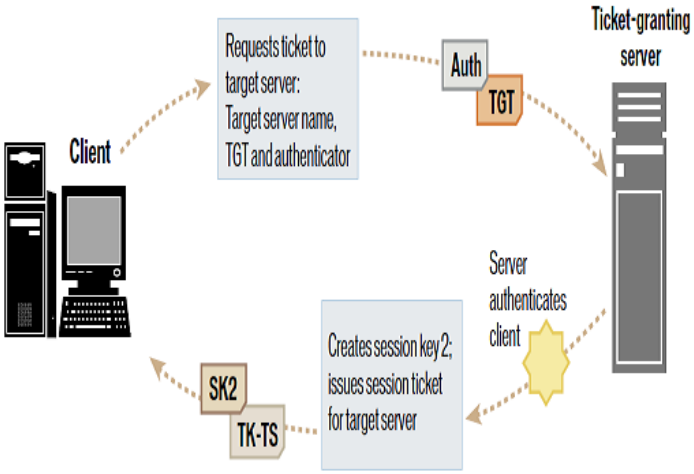

Figure 11: Ticket Granting Service Exchange

3.3 Client/Server Exchange

The message is decrypted by the client to obtain SK2 which is used to encrypt a new authenticator, finally ready to approach the target. Since the authenticator contains plaintext encrypted with SK2, and proves that the client knows the key, the client sends the session ticket (already encrypted with the target server's secret key) and the encrypted authenticator. The encryption of time stamp prevents an eavesdropper from recording both the ticket and authenticator and replay them later [6],[7]. The target server decrypts and verifies the ticket, authenticator, client address and time stamp. For two-way authentication, the target server returns a message consisting of the time stamp plus 1, and is encrypted with SK2. This proves the client that the server actually knew its own secret key and thus could decrypt the ticket and the authenticator.

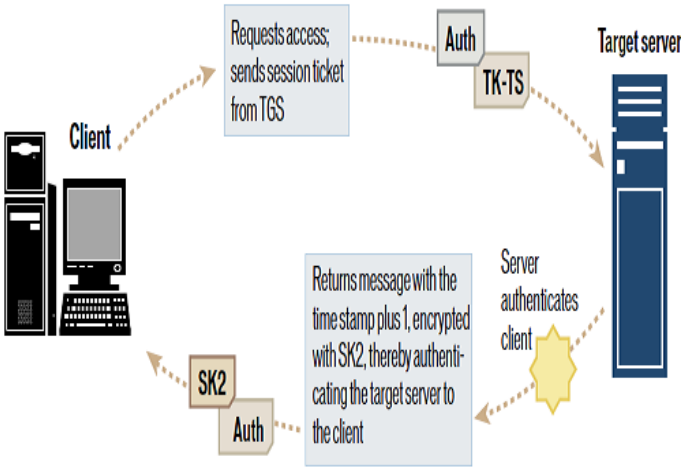

Figure 12: Client Server Exchange

3.4 Secure Communication

Finally the target knows the client is who he claims to be, and the two uses the same encryption key for secure communication. Since, the encryption key is used by the client and the target is same; they assume that a recent message encrypted in that key is originated with the other party as shown in figure 13.

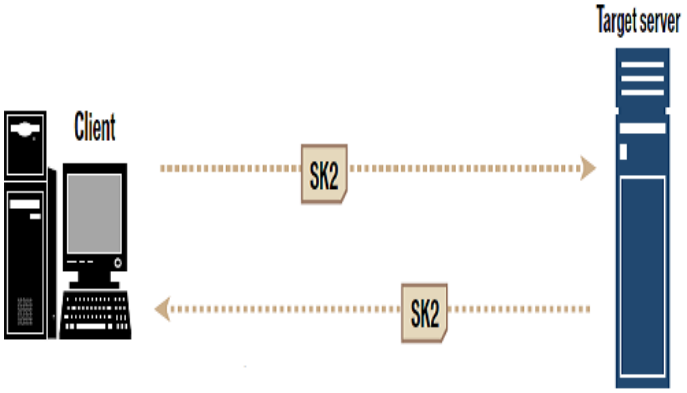

Figure 13: Secure Communication

A resource in the network is accessed only when, the client sends the TGT as it is and requests for a ticket to the particular resource. The authentication data encrypted using the client's session key which is also stored in the TGT is also sent by the client. The TGT is decrypted by KDC to obtain session key to decrypt the authentication data. After the successful decryption of data, the client is validated and the server issues an encrypted ticket for accessing the particular resource. This ticket is sent by the client for service or resource, along with the authentication data encrypted using the session key between it and the resource. The resource decrypts the ticket with the help of its password and extracts the session key and uses it to decrypt the authentication data. If the process works, the resource is allocated [13], [10].

4. Conclusion

Data encryption is a good means of security but it takes time for their operations to be performed which reduces the speed of data transfer and the capabilities of the network. This can be avoided by implementing properly through hardware or software as suggested in this paper. We can minimize these obstacles by the *technological development and theoretical development.* The Kerberos authentication method implemented in this paper is almost unbreakable and totally depends upon Encryption and PKI.

5. References

[1] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005 .
[2] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http:// www. schneier.com/ blowfish.html.
[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.
[4] "Blowfish Encryptio Algorithm.pdf" from pocket brief.net/related/BlowfishEncryption.pdf
[5] "Key Distribution Center and Kerberos Operations " http://www.kerberos.org/software/tutorial .html.
[6] Advanced communications and multimedia security: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, September 26-27, 2002, Portorož, Slovenia
[7] "INTERNET SECURITY: A Jumpstart for systems for systems administartions and IT managers " By Tim Speed, Juanita Ellis
[8] Block Cipher Algorithms", International Journal of Network Security, , Nov. 2007, PP.241–251.
[9] "Digital Signature: Network Security Practices" By Kailash N. Gupta, Kamalesh N. Agarwala, Prateek Amar Agarwala,pp.90-92
[10] Neuman, B.C "Kerberos: an authentication service for computer networks" Communications Magazine, IEEE Volume: 32 Issue:9 On page(s): 33 – 38
[11] Marvin A. Sirbu, John Chung-I Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography," sndss, pp.134, 1997 Symposium on Network and Distributed System Security, 1997
[12] Meyers, R.K.; Desoky, A.H. "An Implementation of the Blowfish Cryptosystem" Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium.pp 346 – 351
[13] "The Kerberos Network Authentication Service" from http://www.networkdictionary.com/rfc.

[14] Moussa, A. "Data encryption performance based on Blowfish" ELMAR,2005. 47th International Symposium .pp 131 – 134.

Authors:

#1 Panchamukesh Chandaka received Bachelors degree in Computer science and Information Technology from JNTUH, Pursuing M.Tech in Information Technology from JNTUK. He is a research scholar in field of Information Security and Software Engineering. He is having experience of 4 Years in the field of Computer Science and Engineering, presently working as Assistant Professor in the department of CSE, Hyderabad Institute of Technology and Management (HITAM), Gowdavally, R.R.Dist.,A.P,INDIA,mukesh_1229@gmail.com.

#2 Professor T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTU. He has 20 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related I.T issues. He is presently Professor and Head, Department of Computer Science and Engineering, Hyderabad Institute of Technology and Management (HITAM), Gowdavally, R.R.Dist., A.P, INDIA. He is nominated as an Editor and Reviewer to 25 International journals relating to Computer Science and Information Technology. He is currently working on research areas which include Digital Image Processing, Digital Watermarking, Data Mining, Network Security and other Emerging areas of Information Technology. He can be reached at tvnrbobby@yahoo.com

#3 A. Vijay kumar, Graduated in **Computer Science and Engineering**. from Jawaharlal Nehru Technological University Hyderabad, India and M.Tech in **Computer Science and Engineering** from Acharaya Nagarjuna University Guntur, A.P, India .He is working presently as Assistant Professor in Department of Computer Science and Engineering , Hyderabad Institute of Technology and Management (HITAM), Gowdavally, R.R.Dist., A.P, INDIA. He has 5 years of Experience. His Research areas include Automata theory, Compiler design, neural networks and Networking. **vijaykanna@live.com**