International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Data Stream UDP using Blowfish Ciphering System

Dr. Taif S. Hasan

Computer Science Department, Al-Mamoon University College
Taif.s.hasan[at]almamonuc.edu.iq

Abstract: ***As UDP does not provide assurance of delivery of packet, reliability and other services, the overhead taken to provide these services is reduced in UDP's operation. Thus, UDP provides low overhead and higher speed. Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control. It is suitable protocol for multicasting as UDP supports packet switching. UDP is used for some routing update protocols like RIP (Routing Information Protocol). There is a need for an efficient fast security issue. The blowfish is simple fast secure algorithm. By adopting the Blowfish method in specific position in the hierarchy of the TCP-IP layer a new secure model will be result.***

Keywords: UDP, Data Stream, Blowfish, Socket, Network, Security

1. Introduction

UDP is commonly used for applications that are "lossy" (can handle some packet loss), such as streaming audio and video. It is also used for query-response applications, such as DNS queries. UDP packets use a 16 bit checksum. It is not impossible for UDP packets to have corruption, but it's pretty unlikely. In any case it is not more susceptible to corruption than TCP.

The adopted encryption method blowfish will be very suitable. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption[1].

2. Papers Review

1) R.K.C. Chang ; K.P. Fung, "Transport layer proxy for stateful UDP packet filtering", Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications, 2002. This paper provides a secure UDP firewall traversal service on the transport layer. [2]
2) K. Rajkumar* and P. Swaminathan, "Combining TCP and UDP for Secure Data Transfer", Indian Journal of Science and Technology, Vol 8(S9), 285–291, May 2015. The aim of this paper is to enchance the security while transferring data between two host through internet. [3]
3) A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement, Mohammad Al-Jarrah, and Abdel-Karim R. Tamimi. They introduce security policy, security control, and data security layer. [4]
4) An Enhanced Security for TCP/IP Protocol Suite, Internation journal of Computer and mobile computing, Dr. M. Anand Kumar, Dr. S, Karthikeyan, propose security architecture for TCP/IP protocol. [5]
5) Karnati Hemanth*, Talluri Ravikiran**, Maddipati Venkat Naveen**, Thumati Ravi***, "Security Problems and Their Defenses in TCP/IP Protocol Suite", International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153. Introduce security problem and the ability to defence. [6]
6) Security Model for TCP/IP Protocol suite. M. ANAnd, Dr S. KrthikeyanKumar Also introduce new layer. [7]
7) In Blowfish algorithm, *e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16*, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83 www.iosrjournals.org www. Ms NehaKhatri – Valmik1, Prof. V. K Kshirsagar2, Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India. [8]

3. The Proposed System

The proposed system includes the use of blowfish encryption technique through the TCP-IP layers. Each TCP/IP layer perform specific function, In order to keep the layers without any undesired modification and effects such as add extra difficulties, make conflict, change the data path, and others; the adopted model add extra layer responsible of security issues. The blowfish will be contained in the extra security layer. Figure 1 show the model structure.

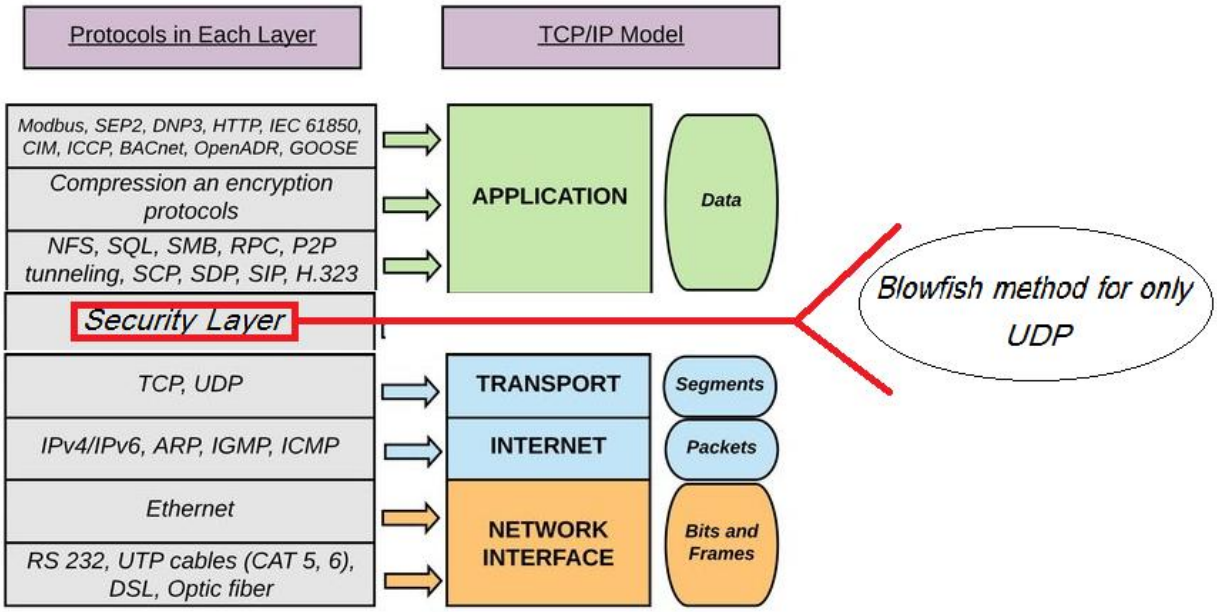

Figure 1: The Proposed Model

Encryption

In cryptography a side channel attack is an attack based on information gained from the physical implementation of a cryptosystem rather than brute force (or) theoretical weakness in the algorithms. For example timing information, power consumption, electromagnetic leaks or even sound can provide extra source of information which can exploit to break the system. Some side- channel attacks requires technical knowledge. As mentioned there are two types of cryptography in use today i.e., symmetric (or) secret key cryptography and asymmetric or public key cryptography. Symmetric is the oldest one. Secret key cryptography involves the use of only one key which is used for both encryption and decryption. [9]

Blowfish Encryption Method

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

The blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption as shown in Figure 2. [10]

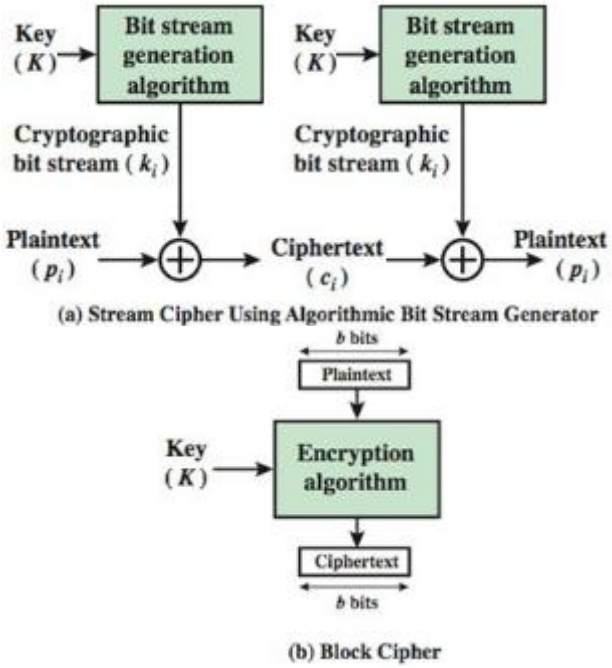

Figure 2: The Block versus Stream Cipher

Blowfish Algorithm

Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. (Not-so-careful implementations, like Kocher, don't increase that time by much.) Longer messages increase computation time in a linear fashion; for example, a 128-bit message takes about (2 x 12) clocks. Blowfish works with keys up to 448 bits in length.

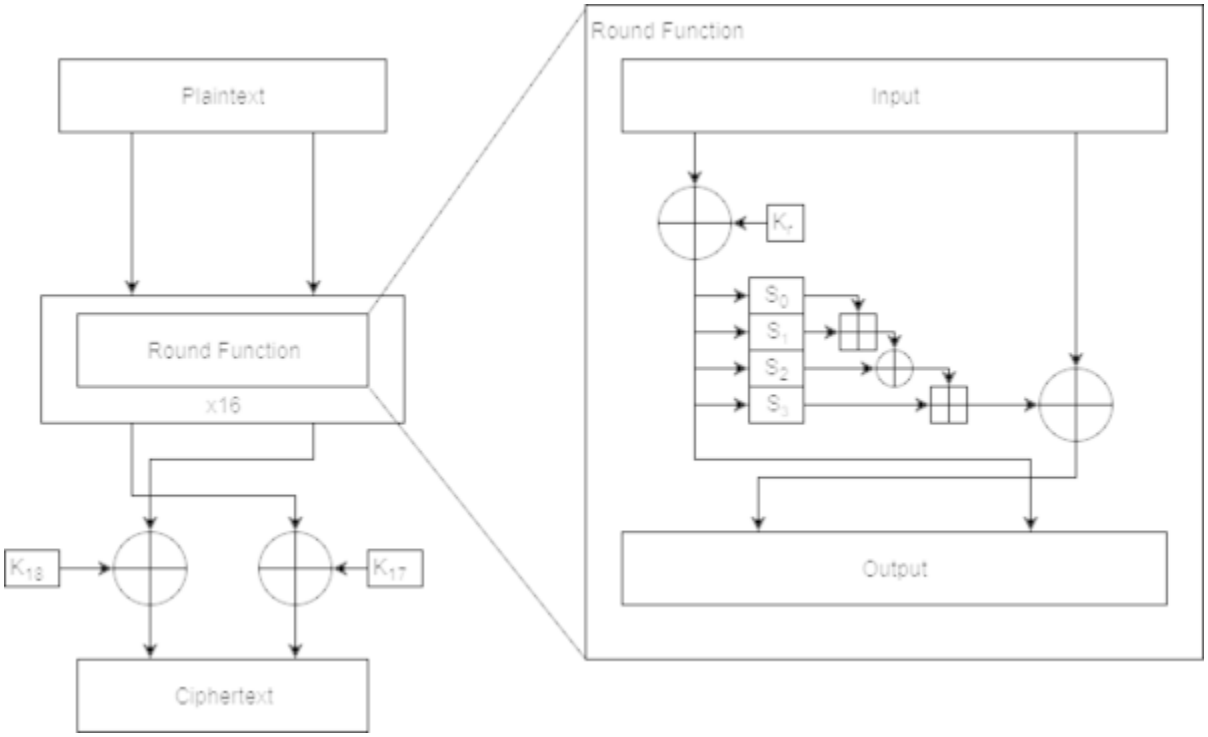

Figure 3: Blowfish algorithm

A graphical representation of the Blowfish algorithm appears in Figure 3. In this description, a 64-bit plaintext message is first divided into 32 bits. The “left” 32 bits are XORed with the first element of a P-array to create a value I'll call P', run through a transformation function called F, then XORed with the “right” 32 bits of the message to produce a new value I'll call F'. F' then replaces the “left” half of the message and P' replaces the “right” half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit cipher text. [11]

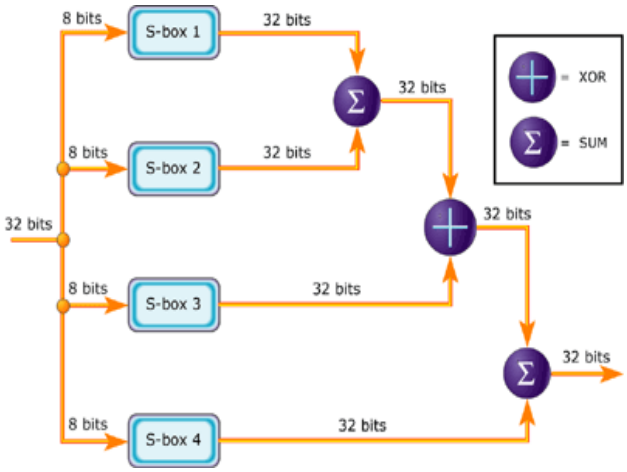

Figure 4: Graphic representation of F

A graphical representation of F appears in Figure 4. The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output.

Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text.

The P-array and S-array values used by Blowfish are pre computed based on the user's key. In effect, the user's key is transformed into the P-array and S-array; the key itself may be discarded after the transformation. The P-array and S-array need not be recomputed (as long as the key doesn't change), but must remain secret.

I'll refer you to the source code for computing the P and S arrays and only briefly summarize the procedure as follows:

- P is an array of eighteen 32-bit integers.
- S is a two-dimensional array of 32-bit integer of dimension 4×256.
- Both arrays are initialized with constants, which happen to be the hexadecimal digits of π (a pretty decent random number source).
- The key is divided up into 32-bit blocks and XORed with the initial elements of the P and S arrays. The results are written back into the array.
- A message of all zeroes is encrypted; the results of the encryption are written back to the P and S arrays. The P and S arrays are now ready for use.

User datagram protocol (UDP)

User datagram protocol (UDP) operates on top of the Internet Protocol (IP) to transmit datagrams over a network. UDP does not require the source and destination to establish a three-way handshake before transmission takes place. Additionally, there is no need for an end-to-end connection.

UDP is faster than TCP, and the simple reason is because its non-existent acknowledges packet (ACK) that permits a continuous packet stream, instead of TCP that acknowledges a set of packets, calculated by using the TCP window size and round-trip time (RTT).

A UDP datagram consists of a datagram header and a data section as shown in Figure 5. The UDP datagram header consists of 4 fields, each of which is 2 bytes (16 bits). The data section follows the header and is the payload data carried for the application.

Unlike TCP, UDP doesn't establish a connection before sending data, it just sends. Because of this, UDP is called "Connectionless". UDP packets are often called "Datagrams". An example of UDP in action is the DNS service.

The User Datagram Protocol (UDP) is a communications standard used for client — server network applications. Engineers use the UDP Test Suite to find bugs and security vulnerabilities in devices prior to deployment. [12]

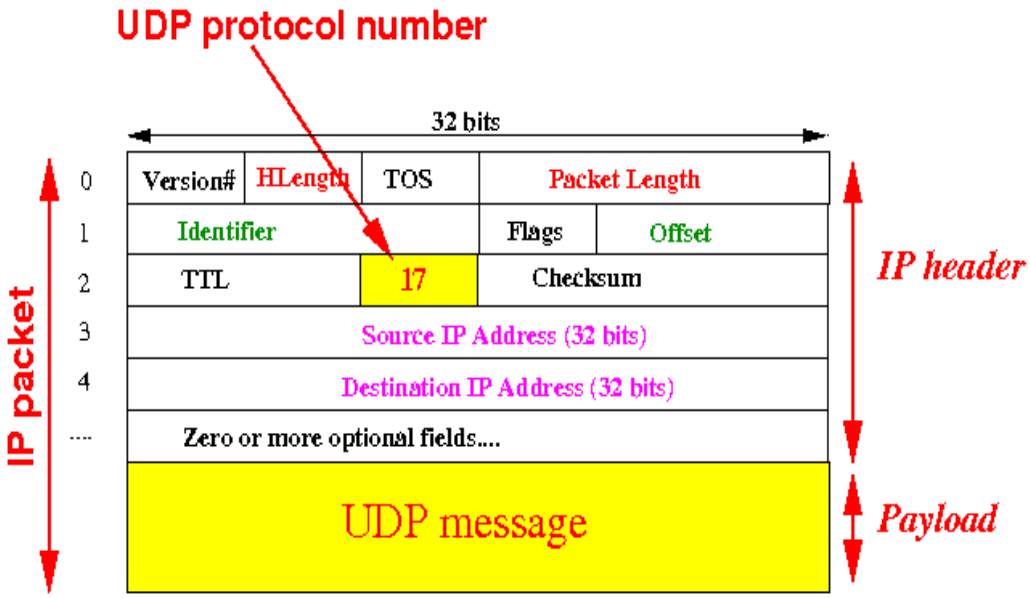

Figure 5: UDP Header

Socket in Computer Network

A **socket** is one endpoint of a **two way** communication link between two programs running on the network. The socket mechanism provides a means of inter-process communication (IPC) by establishing named contact points between which the communication takes place.

Like 'Pipe' is used to create pipes and sockets is created using **'socket'** system call. The socket provides bidirectional **FIFO** Communication facility over the network. A socket connecting to the network is created at each end of the communication. Each socket has a specific address. This address is composed of an IP address and a port number.

Socket are generally employed in client server applications. The server creates a socket, attaches it to a network port addresses then waits for the client to contact it. The client creates a socket and then attempts to connect to the server socket. When the connection is established, transfer of data takes place.

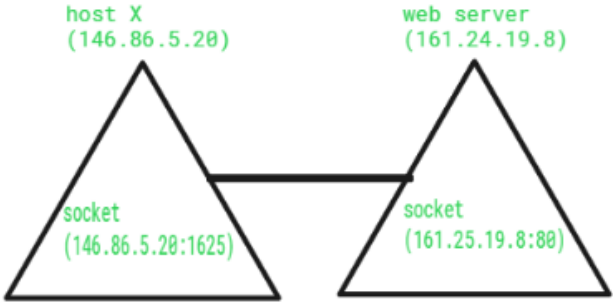

Figure 6: Socket binding

Types of Sockets:

There are two types of Sockets: the **datagram** socket and the **stream** socket.

1) **Datagram Socket:**
   This is a type of network which has connection less point for sending and receiving packets. It is similar to mailbox. The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).
2) **Stream Socket**
   In Computer operating system, a stream socket is type of interprocess communications socket or network socket which provides a connection-oriented, sequenced, and unique flow of data without record boundaries with well defined mechanisms for creating and destroying connections and for detecting errors. It is similar to phone. A connection is established between the phones (two ends) and a conversation (transfer of data) takes place. [13]

4. Result and Conclusion

The result is that UDP can: Achieve higher throughput than TCP as long as the network drop rate is within limits that the application can handle. Deliver packets faster than TCP with less delay. Setup connections faster as there are no initial handshake to setup the connection.

Blowfish is the best suitable encryption method based on the result for the paper [16]. The result give indicator that the blowfish main properties are the speed, low memory need and the high security. The adopted security method serves

many UDP services. Choosing the UDP protocol due to its role in many applications it has wide range of important applications.

1) Figure 7 shows that the blowfish algorithm records the fastest encryption time, and RSA algorithm records the slowest encryption time. Based on the encryption time we will select the blowfish technique for further evaluation.

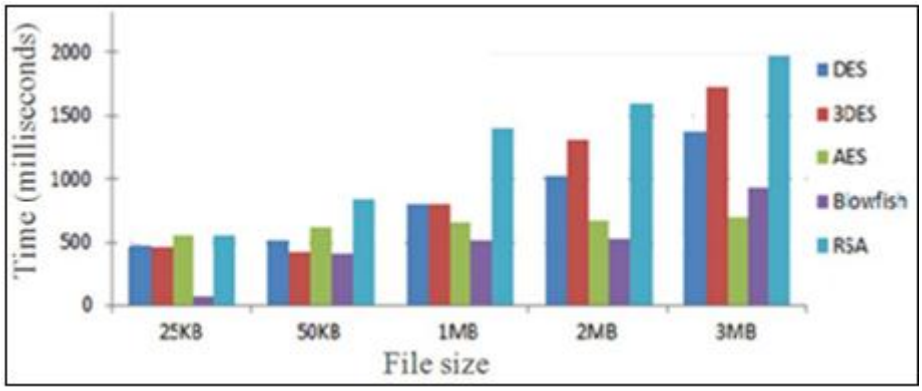

Figure 7: Encryption time vs. File size for DES, 3DES, AES, Blowfish and RSA

2) Figure 8 shows that the decryption time for all algorithms is faster than the encryption time. Also, blowfish algorithm records the fastest decryption time and RSA algorithm records the slowest decryption time. Based on the decryption time feature we will select the blowfish technique to be considered at the next evaluation level.

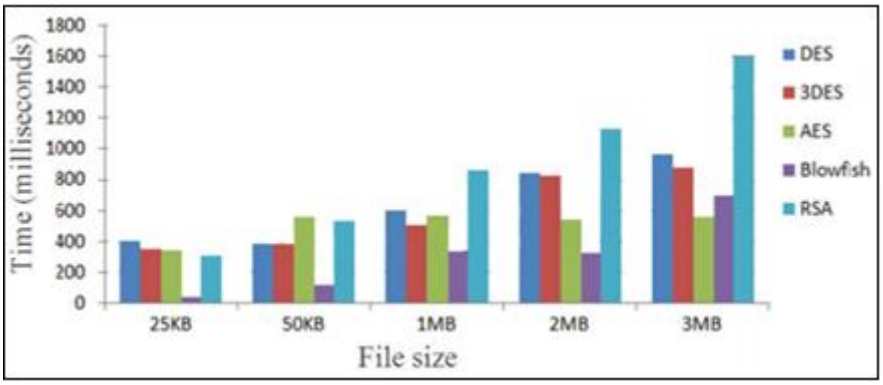

Figure 8: Decryption time vs. File size for DES, 3DES, AES, Blowfish and RSA

3) Up next in the Table 1 presents that memory used for unit operations for all cryptographic techniques that we studied. Blowfish consumed less memory storage than other types, while RSA uses the highest memory.

Table 1: Comparison of memory used

Algorithm	Memory used (KB)
DES	18.2
3DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

4) As the entropy test and final experiment. Table 2 shows that blowfish records the highest average entropy per byte of encryption. That should highlight the blowfish algorithm achievements for consideration of a new security aspect.

Table 2: Average entropy values

Algorithm	Average entropy per byte of encryption
DES	2.9477
3DES	2.9477
AES	3.84024
Blowfish	3.93891
RSA	3.0958

References

[1] The Blowfish Algorithm Simplified, Avinash M Ghorpade1, Harshavardhan Talwar2, Vol. 5, Issue 4, April 2016.
[2] R.K.C. Chang; K.P. Fung, “Transport layer proxy for stateful UDP packet filtering”, Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications, 2002.
[3] K. Rajkumar* and P. Swaminathan, “Combining TCP and UDP for Secure Data Transfer”, Indian Journal of Science and Technology, Vol 8(S9), 285–291, May 2015.

[4] Mohammad Al-Jarrah, and Abdel-Karim R. Tamimi, "A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement".
[5] Dr. M. Anand Kumar, Dr. S, Karthikeyan, "An Enhanced Security for TCP/IP Protocol Suite", International journal of Computer and mobile computing, IGCSMC, Vol. 2, Issue 11, November 2013.
[6] Karnati Hemanth*, Talluri Ravikiran**, Maddipati Venkat Naveen**, Thumati Ravi***, "Security Problems and Their Defenses in TCP/IP Protocol Suite", International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153.
[7] M. ANAnd, Dr S. KrthikeyanKumar, "Security Model for TCP/IP Protocol suite".
[8] Ms NehaKhatri – Valmik1, Prof. V. K Kshirsagar2, "In Blowfish algorithm, e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83 www.iosrjournals.org, Dept. of Comp. Science &Engg. Govt. College of Engg. Aurangabad, India.
[9] Practical Implementation of Blowfish Algorithm for Boosting Security Aspect in Networks, International Journal of Advanced Research in Computer Networking, Wireless and Mobile Communications Volume: 2 Issue: 3 26-Jul-2014, ISSN_NO: 2320-7248.
[10] Blowfish encryption algorithm for information security, January 2015.
[11] Bill Gatliff, "Encrypting data with the Blowfish algorithm July 15, 2003, Technical article.
[12] Margaret Rouse**,** UDP (User Datagram Protocol)
[13] Technical Article for Socket, https://www.geeksforgeeks.org/socket-in-computer-network.
[14] Behrouz A. Forouzan, "Data Communications and Networking", 4th edition, McGraw Hill International Edition, 2007.
[15] Tanenbaum, A. S.; "Computer Network"; 3rd edit; Prentice Hall International Inc; 1996.
[16] Mohammed Nazeh Abdul Wahid*, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", Limkokwing University of Creative and Technology, Post Graduate Centre, Cyberjaya, Malaysia.