www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1318-1323

Dynamic Routing With Security Considerations

Abhinav Srivastava[#1] Amritanshu Srivastava[#2] Gaurav Kumar Mall[#3]

[#]B-Tech Final Year, Department of Computer Science and Engineering,
Institute of Technology And Management, GIDA, Gorakhpur, India.

Abstract-This paper describes dynamic routing with securityusing a cryptographic algorithm which can be used in multiple organization system. The problem of security is the major issues for data communication over worldwide networks. The main objective of this paper is to propose a dynamic routing with security considered using strongest algorithm, such as Blow fish algorithm. Blow fish algorithm provides the strong security from the client to the server system. The dynamic routing avoids two consecutive packets on the same link and updates the routing information from neighbors of the router in the network. The main aim of this paper is a provide strong security from many organizations to a head of the organization, such as Banks, Colleges, Companies, Universities as they need a strong security for data communication. So this paper main issue is to provide strongest security and less time for data transmission from the clients to a server.

Keywords-Blowfish Algorithm, Client-Server system, Distributed computing, Dynamic routing, Multi-Autonomous system, Cryptography system.

1. INTRODUCTION

Various security-enhanced measures have been described to improve the security of data transmission over wired and wireless networks. As the existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their objectives is to defeat various threats over the Internet, including eavesdropping, spoofing, virus ,worms, session hijacking, etc . As Among many well-known designs for cryptography based systems, the P Security (PSec) and the Secure Socket Layer (SSL) are popularly supported and been implemented in many systems and platforms. Although PSec and SSL do greatly improve the security level for data transmission and they unavoidably introduce substantial overheads [8], especially on gateway performance. Data Encryption Standard (DES) /Advanced Encryption Standard (AES) [11] are adopted for encryption/decryption of data transmission in the net work system IPSec [14] .Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is reduce. The main intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission. The set of multiple paths between each source and destination is determined in an online fashion, and extra control message exchanging is needed, propose a secure stochastic routing mechanism to improve routing security. The explored the trading of the security level and the traffic dispersion. They propose data traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. Therefore, we will propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages [9].

2. EXISTING SYSTEM

Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats, virus, and worms over the Internet, including eavesdropping, spoofing, session hijacking etc.
Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) are popularly supported and implemented in many systems and platforms [2]. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads; especially on gateway/host performance and effective network bandwidth. There are some drawbacks in existing system such as

1. Overhead is a maximized, because if any faults in the routing path, we need to setups a new path and, it has less security from client to server.
2. It has not been provided a strongest security and slowly processed of the data transmission from client to server.
3. It was taking a very less time for the data encryption and decryption in the cryptographic system.
4. Administrator intervention is required to maintain changing route information.
5. Requires complete knowledge of the entire network for proper implementation.

3. PROPOSED SYSTEM

Dynamic routing algorithm that could be randomizes delivery paths for data transmission over wired and wireless networks. The objective of this work is to explore a strong security enhanced dynamic routing based on cryptographic algorithm in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets. The dynamic routing provides to avoid two consecutive packets on the

same link and updates the routing information from neighbors' of the router in the network .Advantages Of Proposed System are:

- Our security enhanced in the multiple-autonomous system using a dynamic routing with strong cryptographic algorithm for data transmission.
- Overhead is a minimized, if any faults in the routing path, we need not setups a new path and routing table information, it provides automatically setup of path itself and a strong security from client to server.
- It provides a strong security and fast data encryption and decryption from the client to the destination in the multiple autonomous systems.
- It is a taking a very less time for Bulk encryption of the data processed in the cryptographic system.

4. BASIC DEFINITION AND CONCEPTS

4.1 Distributed computing

Distributed computing utilizes a network of many computers, each accomplishing a portion of an overall task, to achieve a computational result much single computer. In addition to higher level of computing power, distributing computing also allow many users to interact and connect openly. Different form of distributing computing allows for different levels of Openness, with most people accepting that a higher degree of openness in a distributed computing system is beneficial. Many different computers make everything one does while browsing the Internet possible, with each computer assigned a special role within the system. A home computer is used, for example, to run the browser and to break down the information being sent, making it accessible to the end user [17]. A server at your Internet service provider acts as a gateway between your home computer and the greater Internet. These servers speak with computers that comprise the domain name system, to help decide which computers to talk too based on the URL the end user enters. Early distributed systems worked over short distances, perhaps only within a single room, and all they could really do was to share a very few values at set points of the computation. The larger number of computers has only partially helped; while it has meant that it is possible to use more total computation and to split the problems into smaller pieces (allowing a larger overall problem), it has also increased the amount of time and effort that needs to be spent on communication between the computers, since the number of ways to communicate can increase (see Figure 1).

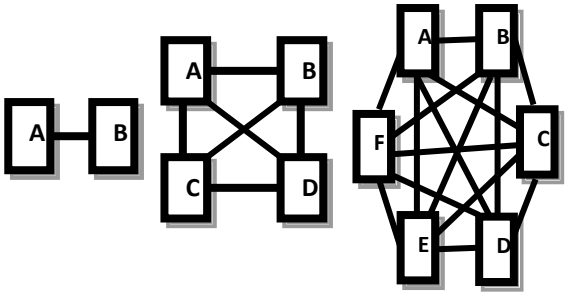

Fig.1 The growth in the number of links as the number of computer goes up.

There are, of course, ways to improve communication efficiency, for instance by having a few computers specialize in handling the communications (like a post office) and letting all others focus on the work, but this does not always succeed when the overall task requires much communication.

4.2Autonomous system

An autonomous system (AS)—otherwise known as a routing domain—is a collection of routers under a common administration. Typical examples are a company's internal network and an ISP's network. Because the Internet is based on the autonomous system concept, two types of routing protocols are required: interior and exterior routing protocols.

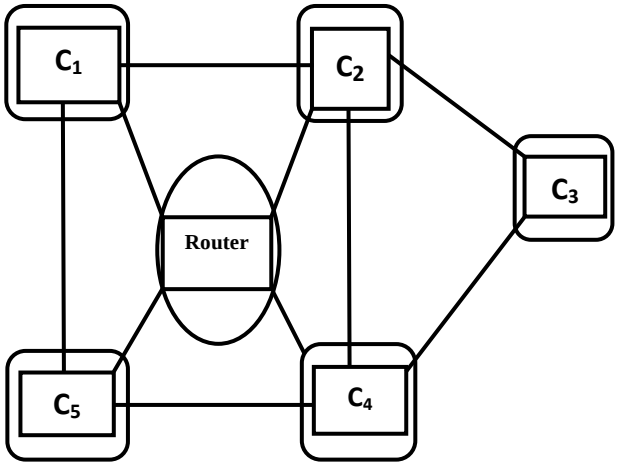

Fig. 2 Autonomous system

These protocols are Interior gateway protocols (IGP): Used for intra-autonomous system routing, that is, routing inside an autonomous system IGPs are used for routing within a routing domain, those networks within the control of a single organization [18]. It is a using for single network system such as, colleges, institutes, Banks, small companies these are include in the autonomous system.

4.3 Multi-Autonomous system

BGP is used for inter-autonomous system routing, that is, routing between autonomous systems a collection of a more than one Autonomous system under a different administration The main focus is on Border Gateway Protocol (BGP)[18], the protocol used to share information between Autonomous systems, and the security vulnerabilities in it.Characteristics of BGP in the Multi-Autonomous systemBGP is different from other routing protocols in several ways. Most important being that BGP is neither a pure distance vector protocol nor a pure link state protocol. Let's have a look at some of the characteristics that stands BGP apart from other protocols.

- **Inter-Autonomous System Configuration:** BGP's primary role is to provide communication between two autonomous systems.

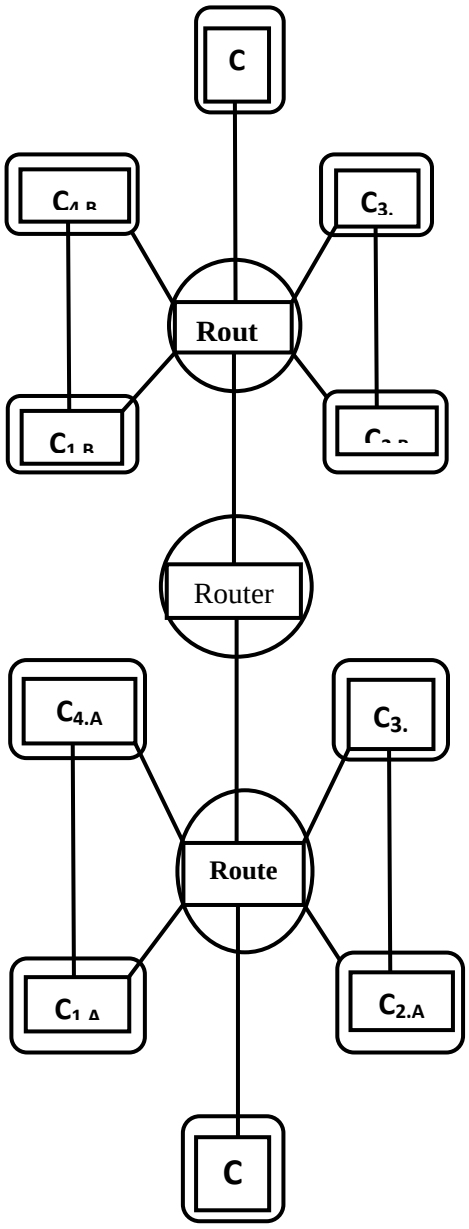

Fig.3 Multi-Autonomous system

- **Next-Hop paradigm:** Like RIP, BGP supplies next hop information for each destination.
- **Coordination among multiple BGP speakers within the autonomous system**: If an Autonomous system has multiple routers each communicating with a peer in other, Autonomous system, BGP can be used to coordinate among these routers, in order to ensure that they all propagate consistent information.
- **Path information**: BGP advertisements also include path information, along with the reachable destination and next destination pair, which allows a receiver to learn a series of autonomous system along the path to the destination.
- **Policy support**: Unlike most of the distance-vector based routing, BGP can implement policies that can be configured by the administrator [19]. For Example, a router running BGP can be configured to distinguish between the routes that are known from within the Autonomous system and that which are known from outside the autonomous system.
- **Runs over TCP**: BGP uses TCP for all communication. So the reliability issues are taken care by TCP.
- **Conserve network bandwidth**: BGP doesn't pass full information in each update message. Instead full information is just passed on once and thereafter successive messages only carries the incremental changes called deltas.
  By doing so a lot of network Bandwidth is saved. BGP also conserves bandwidth by allowing sender to aggregate route information and send single entry to represent multiple, related destinations.
- **Support for CIDR**: BGP supports classless addressing (CIDR). That it supports a way to send the network mask along with the addresses.
- **Security:** BGP allows a receiver to authenticate messages, so that the identity of the sender can be verified.

4.4 Client-Server System

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and operate over service requesters, called clients. Often clients and servers a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients [20]. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.This is client/server computing described. To truly understand how much of the Internet operates, including the Web, it is important to understand the concept of client/server computing. The client/server model is a form of distributed computing where one program (the client) communicates with another program (the server) for the purpose of exchanging information. A typical client/server interaction goes like this:

- The user runs client software to create a query.
- The client connects to the server.
- The client sends the query to the server.
- The server analyzes the query.
- The server computes the results of the query.
- The server sends the results to the client.
- The client presents the results to the user.
- Repeat as necessary.

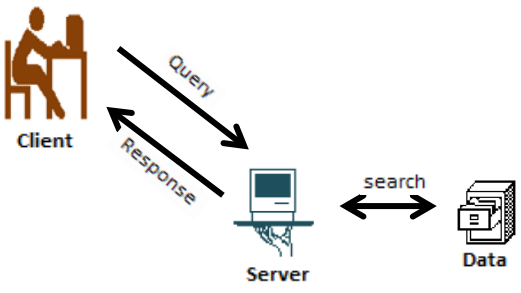

Fig.4 A typical client/server interaction

4.5 Dynamic routing

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. Instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. It's this intelligent and hands-off approach that makes dynamic routing so useful.

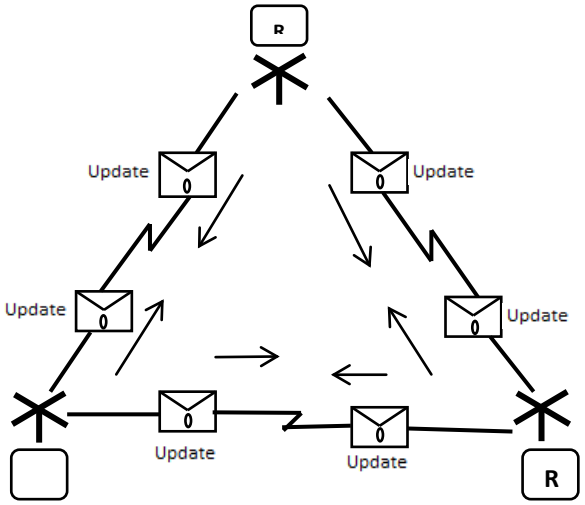

Fig5. Routers Dynamically Pass Updates.

Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing [18].These variations take into account differences in reliability, speed of convergence, and other similar factors. For more information on these administrative distances, see —Multipath routing and determining the best route on. Characteristics of dynamic routing are

1. **Router Memory Required**: for larger tables
2. **Overhead:** Varying amounts of bandwidth used for routing protocol updates .
3. **Scalability:** Very scalable, better for larger networks .
4. **Robustness**: Robust traffic routed around failures automatically .
5. **Convergence:** Varies from good to excellent

5. CRYPTOGRAPHY SYSTEM

Cryptography is the science of encrypting and decrypting written communication. It comes from the Greek word —kryptos, meaning hidden, and —graphia, meaning writing. Cryptanalysis is the process of trying to decrypt encrypted data without the key [1]. A system that provides encryption and decryption is referred to as a cryptosystem.

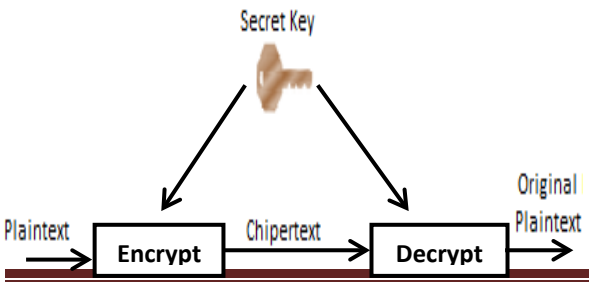

Fig 6.Diagram of symmetric (single key) cryptography

- **Plain text:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm**: This algorithm performs various substitutions and transformations on the plain text.
- **Secret key:** the secret key is also input the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Cipher text:** this is the scrambled message produced as output. t depends on the plain text and the secret key. For a given message, two different keys will produce two different cipher texts.
- **Decryption algorithm:** this is essentially the encryption algorithm run in reverse. It takes cipher text and the same secret key and produces original plain text.

5.1 Blow fish algorithm

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. In the following two sections we would explain in details the two parts of the blowfish algorithm which they are: data encryption & key expansion

- **Data encryption:** The input is a 64-bit data element, x. Divide x into two 32-bit halves: xL, and xR.

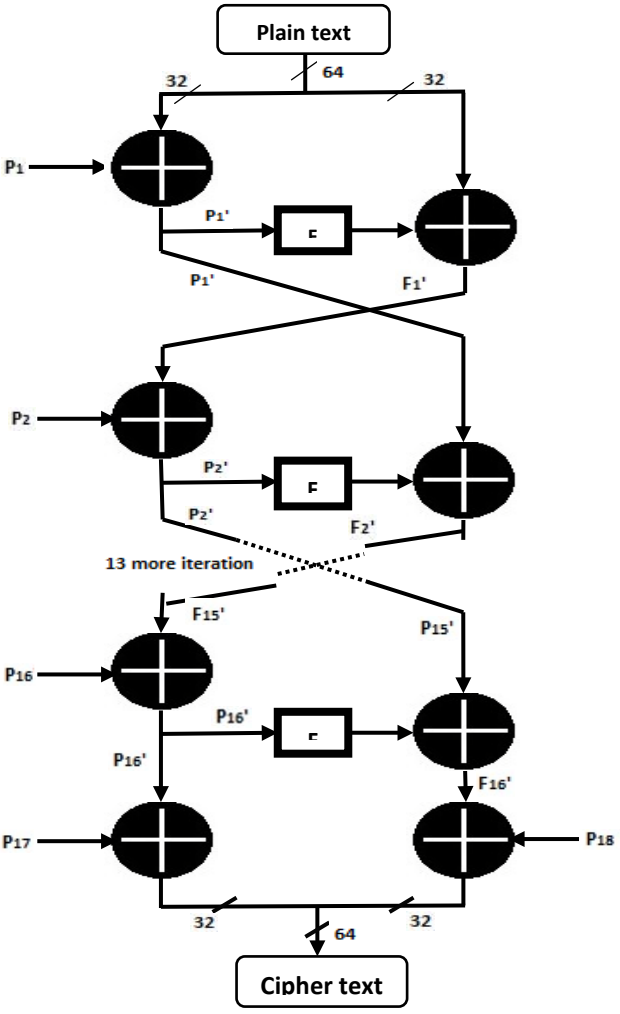

Fig 7.Blow fish algorithm

- **Key expansion:** Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several sub key arrays totalling 4168 bytes. Blowfish has 16 rounds. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution.

A shown in the figure 6, the description of the blow fish algorithm 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 XOR ed 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.

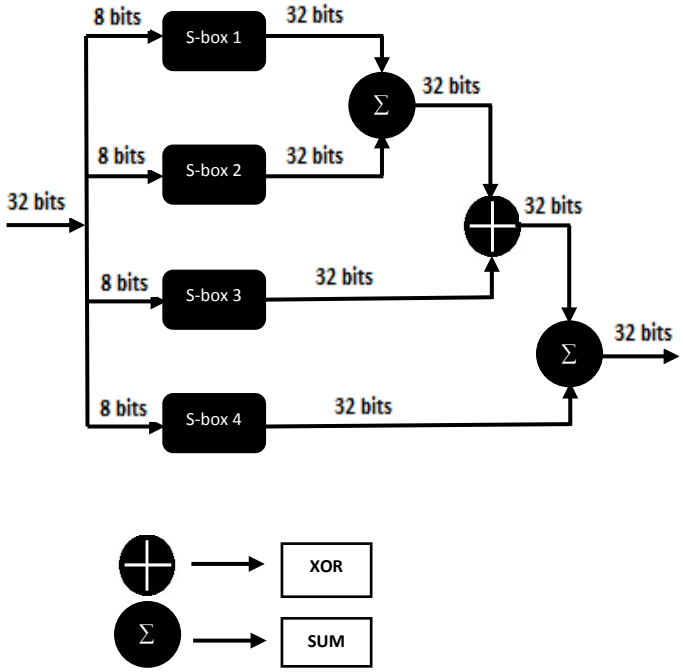

Fig 8.Graphic representation of F

It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Feistel ciphers are a special class of iterated block ciphers where the cipher calculated from the plaintext by repeated application of the same transformation function [21]. A shown in the above figure7.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 refers you to the source code for computing the P and S arrays and only briefly summarizes the procedure as follows:

P is an array of eighteen 32-bit integers.

1. S is a two-dimensional array of 32-bit integer of dimension 4x256.
2. Both arrays are initialised with constants, which happen to be the hexadecimal digits of π (a pretty decent random number source).
3. 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.
4. A message of all zeros 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.

5.2 Dynamic routing with Blow fish algorithm in the Multiple Organization system

Blow fish algorithm provides a strongest security from source to destination with the fast data processed in the multiple organization system. Now, days security is a more important for data communications from client to server in any fields. The security-enhanced dynamic routing algorithm based on Blow fish algorithm widely supported in existing wired and wireless networks.

The different organization system needs high security for data transmission from one organization to other organizations system. If security has not a strong in the any organization system ,any one hackers the their important information to lose the organization information ,so we need a strong security for data communications between client and server in the organization system ,so we have to choose a strong security and fast encryption for data processing in the organization system, so we are using a strong security algorithm for data communication between source and destination, such as Blow fish algorithm is a strength of key length more than DES algorithm. As shown in the figure 8, it shows the dynamic routing with security using Blow fish algorithm in the multiple organization system. In that figure can be divided into three kinds of figures shows different ,Clients Routers and Servers these are using for different organizations system in different kinds of password are maintaining because any one can hackers their important information, so they need strongest security for data communication between clients and server. Now day's security is a more important for data transmission in the autonomous system. As shown in the figure (A.1), it consists of number of clients are connected to server via router. We are used the Blow fish algorithm for security purpose for data communication from source to destination, in that algorithm considered secrete key that key is a sharing only sender and receiver for their data can be encryption and decryption

process . The sender key and receiver key should be match then the data will be successfully sent to their desired destination, so this organization depends on secrete key system. As shown in the figure (B.1),this also same algorithm are used for security purposes of the data transmission form client to server. The sender key and receiver key should be match the data will be successfully sent to their desired destination, so this organization depends on secrete key system. Figure.1, (A.1) and (B.1) both are different organizations system to connected to Head of the organization system. They are maintaining different Passwords and IP address Port number of the their network for security purposes ,because no one hackers their organization information ,so we are using a Blow fish algorithm .The both organizations are combined in to connected via router. That router is connected to other of the main Head of the organization for data communication between different organizations system. The Head of the organizations are also maintaining a secrete key for data communication of the different organizations .In the Head of the organization is also maintaining secrete key ,that key must be match between different kinds of the organization keys ,if head of the organization key should not match with different organizations ,then data will not be successfully send to destination.

6. CONCLUSION

The main contribution of the paper is in proposing a security-enhanced dynamic routing with security based on cryptographic algorithm, such as Blow fish algorithm in the Multi-Organization system. The main proposed of the paper a dynamic routing with strong security algorithm, such as Blow fish algorithm, which is provided a fast and strong security from source to destination based on key length of algorithm. The dynamic routing could be used to a randomization of delivery paths from client to sever in the wire and wireless network. It avoids the path similarity and two same packets on the same path among the different paths in the network. This algorithm is a more performance than other algorithms such as DES, 3DES and AES .In this paper main objective is provide a fast data encryption and decryption and strong security for data communication in the multiple-organization system. The objective of the paper is a taking very less time for data processing to other algorithm and cost also very less to implement any kinds of the large networks ,we may use this algorithm, so The dynamic routing with security for data transmission in the multiple-organizations system.

7. REFERENCES.

1. John E. Canavan, Artech House Boston • London —Fundamentals of Network Security‖ http://www.artechhouse.com
2. Chin-Fu Kuo, Member, IEEE, Ai-Chun Pang, Member, IEEE, and Sheng-Kun Chan —Dynamic Routing with Security Considerations‖ IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 1, JANUARY 2009.
3. K. Becker, U. Wille, —Communication Complexity of Group Key Distribution,‖ Proc.5th ACM Conference on Computer &Communicatios Security, pp. 1-6, San Francisco, CA, November 1998.
4. M. Steiner, G. Tsudik, M. Waidner, —Diffie-Hellman Key Distribution Extended to Groups,‖ 3rd ACM Conference on Computer & Communication Security, pp. 31-37 ACM Press, 1996.
5. W.Diffie, M.Hellman,‖New directions in cryptography‖, IEEE Trans. On Information Theory, 22(1976), 644-654.
6. Ingemarsson, D.Tang, C.Wong. —A Conference Key Distribution System‖, IEEE Trans. on Information Theory, 28(5): 714-720, Sept. 1982.
7. M.Burmester, Y.Desmedt. —A Secure and Efficient Conference Key Distribution System‖, Advances in Cryptology– EUROCRYPT‘94, Lecture Notes in Computer Science. Springer- Verlag, Berlin, Germany.
8. Y. Kim, A. Perrig, G. Tsudik, —Simple and Fault Tolerant Key Agreement for Dynamic Collaborative Groups,‖ Proc. 7th ACM Conf. on Computer and Communication Security (CCS 2000), pp. 235-244.
9. J. Katz, M.Yung, — Scalable Protocols for Authenticated Key Exchange—, Advances in Cryptology - EUROCRYPT‘03, Springer-Verlag, LNCS Vol 2729, pp. 110-125, Santa Barbara, USA.
10. J.Katz, R.Ostrovski, A. Smith, —Round Efficiency of Multi-Party Computation with a Dishonest Majority‖, Advances in Cryptology, EUROCRYPT‘03, LNCS Vol. 3152, pp.578-595, Santa Barbara, USA.
11. Y.Amir, Y.Kim, C.Rotaru, J.Schultz, G.Tsudik, —Exploring Robustness in Group Key Agreement‖, Proc. of the 21th IEEE Int‘l Conference on Distr. Computing Systems, pp. 399-408, Phoenix, AZ, April 16-19, 2001.
12. Y.Amir, Y.Kim, C.Rotaru, J.Schultz, J.Stanton, G.Tsudik, —Secure Group Communication using Robust Contributory Key Agreement‖., IEEE Trans. on Parallel and Distributed Systems, Vol. 15, number 5, pp. 468-480, May 04.
13. W. Lou and Y. Fang, —A Multipath Routing Approach for Secure Data Delivery,‖ Proc. IEEE Military Comm. Conf. (Mil2om), 2001.
14. W. Lou, W. Liu, and Y. Fang, —SPREAD: Improving Network Security by Multipath Routing,‖ Proc. IEEE Military Comm. Conf. (MilCom), 2003.
15. S.Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, —Enhancing Security via Stochastic Routing,‖ Proc. 11th Int‘l Conf. Computer Comm. and Networks (ICCCN), 2002.
16. Lepakshigoud T —Dynamic Routing with security using a DES algorithm‖ NCETIT-2011
17. Donal — Distributed system‖Connexions IBC Plaza Houston on Aug 25, 2009
18. The activities and labs available in the companion Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide (ISBN 1-58713-204-4) http://www.traceroute.org.
19. S. Kent, C. Lynn and K. Seo. Secure Border Gateway Protocol (S-BGP) IEEE Journal on Selected Areas In Communications, Vol. 18,No.4,April2000.http://www.comsoc.org/sac
20. Chris Mayer —Introduction to Client/Server Systems‖ ANSA wise 24th April 1995.
21. [21] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer Verlag, 1994, pp. 191-204. , www.eetindia.com .