iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Dynamic Routing with Security using a Blow fish algorithm in the Network System

Lepakshigoud. T[1], Dr. Nagaraj B Patil[2]
[1]Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India
[2] Computer Science and Engineering, Government Engineering of College, Raichur, Karnataka, India.

Abstract:-In this paper is about encryption and decryption of the text, image, audio, video using a secret key block cipher which is for the dynamic routing with security using a cryptographic algorithm in the network system. The main objective of the work is a dynamic routing with security considered using strongest key length such a blowfish algorithm. It avoids two consecutive packets on the same link/path in the network system, our experiments shows that use of iterative approach enhances the security provided by a algorithm when compared to the non-iterative approach and a strongest security and less time for data transmission from source to the destination in the network system.
Keywords: Algorithms, Blowfish, Cryptography, Dynamic routing, Network system.

I. INTRODUCTION

In the present scenario almost all, the data is transfer over computer networks due to which it is vulnerable to various kinds of attacks to make the data secure from various attacks and for the integrity of data, we must encrypt the data before it is transmit or stored [1]. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals) , geographical areas(in research),enemy positions (in defense), product , financial status, most of this information is now collected and stored on electronic computers and transmitted across network system

If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war wrong treatment etc. Protecting confidential images is an ethical and legal requirement, we store information in computer system in the form of files. File is considered as a basic entity for keeping the information, therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is word wide accepted fact that securing file data is very important, in today is computing environment. Cryptography is a method of storing and transmitting data, It is a science of protecting information by encoding into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. The security has become one of the major issues for data communication over worldwide networks. The objective of the work is a dynamic routing with security considered using strongest algorithm, such as Blowfish algorithm, which is provide the strong security from the client to the server system. 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. To encrypt the data various cryptographic algorithms such DES, 3DES, blowfish, AES, etc are used ,So we are implementing blowfish algorithm which is strongest and fastest in data processing/storing compare to other algorithms which is mentioned above. Blowfish algorithm is highly secured because it has longer key length (more no of key size).The philosophy of proposal algorithm is to use the full menu of "Strong operations" supported in modern computers to achieve better security properties and provide high speed.

The main aim behind the design of this proposal is to get the best security/performance tradeoff over existing ciphers, the various security-enhanced measures have been proposed to improve the security of data transmission over wired and wireless networks. 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 over the Internet, including eavesdropping, spoofing, virus, worms, session hijacking, etc. Among many well-known designs for cryptography-based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) are popularly supports and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads [9], especially on gateway/host performance and effective network bandwidth.

©IJRASET: All Rights are Reserved

When Data Encryption Standard (DES) /Advanced Encryption Standard (AES) [12] has adopted for encryption/decryption for data transmission in the net work system IPSec [15].Another alternative for security-enhanced data transmission is 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 slim. The 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 propose data traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided the set of data delivery paths is discovered in advance, although excellent research results have proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion for those online path-searching approaches the discovery of multiple paths involves a significant number of control signals over the Internet. On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration. [10] Therefore, we will propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages.

II. RELATED WORK

Numerous works are going on different applications depends on different algorithms and Technologies in that field, we are using a Dynamic routing with security algorithms such as a Blow fish algorithm in the multiple organization system. John E. Canavan Fundamentals of Network Security More recently, Yahoo, Amazon.com, eBay, and some other popular World Wide Web (WWW) sites were targets of what appears to have been a coordinated [1],"denial-of-service" attack.. Becker et al. [2]. Derived lower bounds for contributory key generation systems for the gossip problem and proved them realistic for Diffie-Hellman (DH) based protocols Steiner et al [3]. Proposed the basic DH distribution [4] extended to groups from the work. Where three new protocols are presented: GDH.1-2-3. Ingemarsson et al [5] Presented another efficient DH-based KA scheme, ―ING‖, logically implemented on a ring topology Bur ester et a. Introduced a new GDH protocol,[6] denoted as BD (very efficient in terms of round complexity), Kim et al. [7] Proposed another hybrid DH-based KA scheme is TGDH introduced is an efficient protocol that blends binary key trees with DH key exchanges. Katz et al[8, 9] Proposed to improve on existing KA schemes either by rendering them more scalable or by enhancing their security against various kinds of attacks, the described algorithms are implemented on logical graphs or address wire-line networks. Amir et al. [10, 11] Focused on robust KA, and attempt to make GDH protocols fault tolerant to asynchronous network events. However, their scheme is designed for the Internet, and requires an underlying reliable group communication service and message ordering, so that preservation of virtual semantics is guaranteed. Lou et al**.** [12, 13] proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed. Bo hacek et al. [14] proposed a secure stochastic routing mechanism to improve routing security. Yang and Papavassiliou, [15] Explored the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered. Given a graph for a network under discussion, a source node, and a destination node, the problem is to minimize the path similarity without introducing any extra control messages, and thus to reduce the probability of eavesdropping consecutive packets over a specific link. The security has become one of the major issues for data communication over wired and wireless networks. Different from the past work on the designs of cryptography algorithms and system infrastructures [16],a dynamic routing algorithm that randomizes delivery paths and chooses the best path for data transmission.

III. STUDY OF BLOWFISH ALGORITHM AND DYNAMIC ROUTING

A. Blowfish Algorithm

The data transformation process uses the Blowfish Algorithm for Encryption and Decryption, respectively. The details and working of the algorithm are given below. It is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm 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. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher [18]. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

©IJRASET: All Rights are Reserved

1) Description of the algorithm

Blowfish is a variable-length key, 64-bit block cipher.

The algorithm consists of two parts: a key-expansion part and a data- encryption part.

Key expansion: converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes.

Data encryption: occurs via a 16-round Feistel network [fig1]. Each round consists of a key dependent Permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Encryption:

Blowfish has 16 rounds.

The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL and xR to get the cipher text. Pocket Brief 5 of 7 Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in there verse order[21]. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

2) Feistel Networks

A Feistel network is a general method of transforming any function (usually called an F function) into a permutation [fig1]. It was invented by Horst Feistel and has been used in many block cipher designs. The working of a Feistal Network is given below:

a) Split each block into halves

b) Right half becomes new left half

c) New right half is the final result when the left half is XOR'd with the result of applying *f* to the right half and the key.

d) Note that previous rounds can be derived even if the function *f* is not invertible.

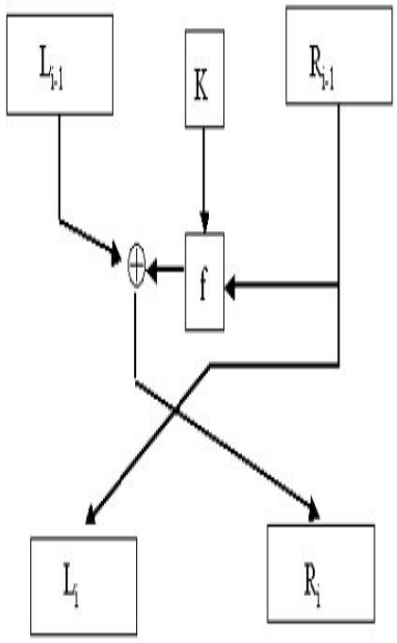


Fig 1: Feistel Networks.

©IJRASET: All Rights are Reserved

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

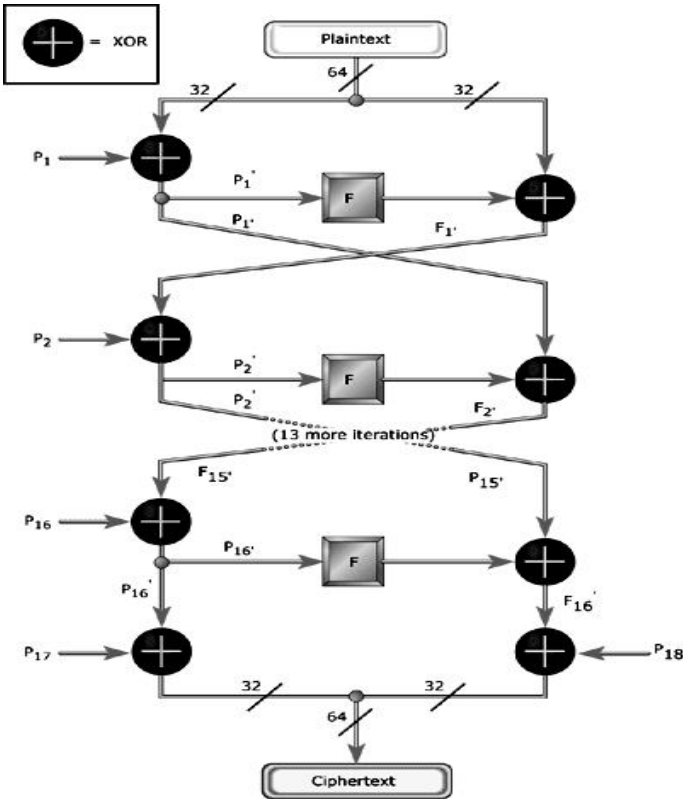


Fig.2 Process of Blow fish Algorithm.

B. Dynamic Routing

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So 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 [fig3]. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing [19]. 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 “route on.

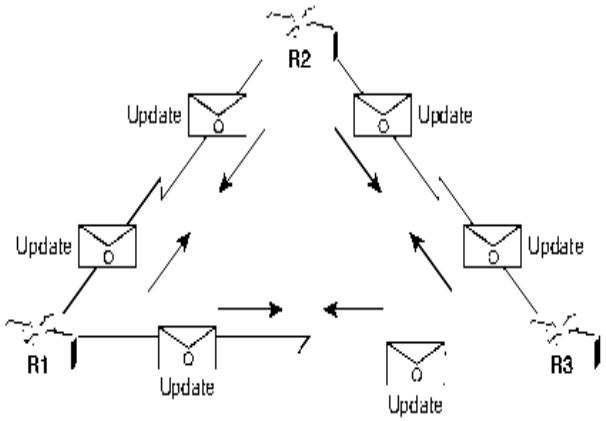


Fig.3 Dynamically pass updates via router.

©IJRASET: All Rights are Reserved

1) The router sends and receives routing messages on its interfaces.
2) The router shares routing messages and routing information with other routers that are using the same routing protocol.
3) Routers exchange routing information to learn about remote networks.
4) When a router detects a topology change, the routing protocol can advertise this change to other routers
5) Dynamic routing advantages are as follows:
6) Administrator has less work in maintaining the configuration when adding or deleting networks.
7) Protocols automatically react to the topology changes.
8) Configuration is less error-prone.
9) More scalable; growing the network usually does not present a problem

IV. PROPOSED SYSTEM

This research proposes a new improvement to the blowfish algorithm, the proposed improvement makes use of the new system is a binary and digit operations of the algorithm uniquely define the mathematical steps required to the transform of the data into a cryptographic cipher and also to transform the cipher back to the original form, here introduced a new method to enhance the performance of the blowfish algorithm is introduced to our network system. This is a done by replacing the predefined digit and binary operations vice-versa applied during nearly very less steps of the blowfish algorithm/binary algorithm by a new operation depends on the binary and digit operations of the given a plaintext[fig4].

This replacement adds a new level of protection strength and more robustness against breaking the methods and takes very less time to complete the given work in the network system. Shown in the figure the modification of the blow fish algorithm using a binary and digit operation to the enhance security from the source to destination in the network system to using different types of the operations done by the mathematical opertion such as digit and binary operations from the plain text to cipher text then vice-versa**.**

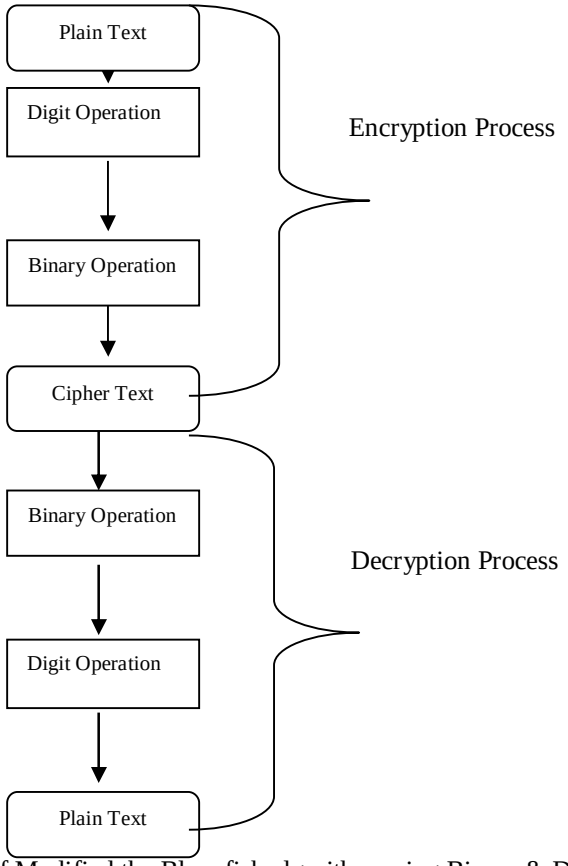


Fig: 4 Design of Modified the Blow fish algorithm using Binary & Digit operations.

©IJRASET: All Rights are Reserved

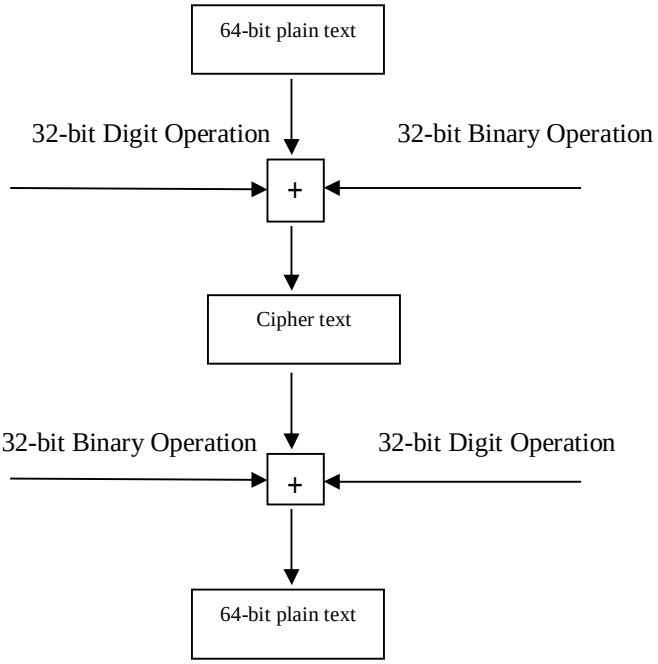


Fig: 5 Input and Output of the "+" operation in the Blow fish algorithm.

To increase the security and key space, that makes the encryption algorithms more robustness to the intruders, a new manipulation bits process has been added in by using different type of operations for manipulation bits process work on 2- states, while the traditional binary process (OR) work on (0, 1) bits only. The symbol + has been used to refer to the operator that execute this process shown in [fig5], the first one specify the 64-bit number that should be used to calculate the result among the 2 parts, the 32-bit inputs define the lift and right number in the specified where the cross point of them gives the result.

Example for + operation, this operation need 2 inputs, first one specify the 32-bit number that should be used to calculate the result among the as shown in figure, the other 2 inputs define the lift and right number in the specified table where the cross point of them gives the result this result is in 16 digits.

Input in 32 bit binary format 10010111010100101010011111010001001

which is converted into the number 2 1 1 3 1 1 0 2 2 2 1 3 2 2 0 2 1,Shown in the above figure from the plain text to the cipher text with help of the operations such as digit or binary operations using a plus sign to converted plain text to cipher text.

V. CONCLUSION

The main contribution of the work is proposing a security enhanced dynamic routing with security based on cryptographic algorithm such as blow fish algorithm of the binary and digit operations in the network system. The blow fish algorithm is supposed to be better algorithm which is provides a fast and strong security from the source to the destination based on the key length of algorithm. The dynamic routing could be used to the randomization of delivery paths from client to server in the wired and wireless network system .It avoids the path similarity and two same packets on the same path among the different paths in the network. The objective of the work is a taking very less time for data encryption and decryption process in the network, which is a main objective of the algorithm, is less cost and more performance of the security provided in the network system.

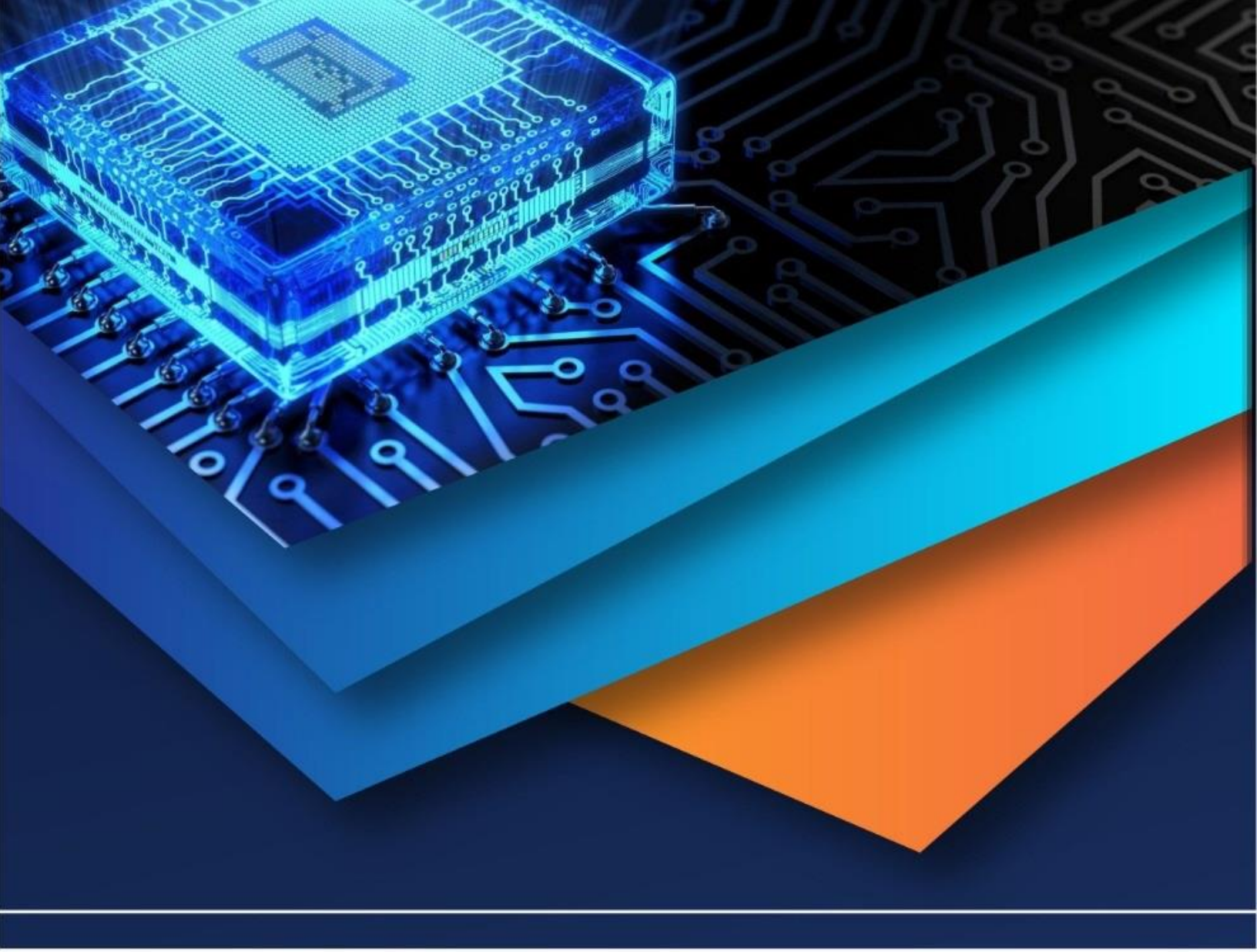
REFERENCES

[1] Irfan.Landge1, Burhanuddin Contractor2, Aamna Patel3 and Rozina Choudhary4- Image encryption and decryption using blowfish algorithm, World Journal of Science and Technology 2012, 2(3):151-156,ISSN: 2231 – 2587
[2] John E. Canavan, Artech House Boston • London ―Fundamentals of Network Security‖ http://www.artechhouse.com
[3] 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.
[4] 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.

©IJRASET: All Rights are Reserved

[5] 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.
[6] W.Diffie, M.Hellman, New directions in cryptography‖, IEEE Trans. On Information Theory, 22(1976), 644-654.
[7] Ingemarsson, D.Tang, C.Wong. ―A Conference Key Distribution System‖, IEEE Trans. on Information Theory, 28(5): 714-720, Sept. 1982.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] W. Lou and Y. Fang, ―A Multipath Routing Approach for Secure Data Delivery,‖ Proc. IEEE Military Comm. Conf. (Mil2om), 2001.
[15] W. Lou, W. Liu, and Y. Fang, ―SPREAD: Improving Network Security by Multipath Routing,‖ Proc. IEEE Military Comm. Conf. (MilCom), 2003.
[16] 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.
[17] Lepakshi Goud T ―Dynamic routing with security using a DES algorithm‖ NCETIT-2011.
[18] 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
[19] Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide (ISBN 1-58713-204-4)

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)