Incorporated File Replication and Consistency Maintenance in P2P Systems with Sanctuary

B. Srinivasa Rao[1], B.Krishna [2], V. Krishna Pratap [3], A. Divya[4]

Department of Computer Science & Information Technology, Sri Sarathi Institute of Engineering and Technology, Nuzvid, Jntuk, A.P, INDIA

[1]srinuprec@gmail.com, [2]krishnab2021@gmail.com, [3]pratapv9@gmail.com, [4]divya501.cute@gmail.com

***Abstract*— In peer-to-peer file sharing systems, file replication and consistency maintenance are broadly used techniques for high system recital. Despite significant interdependencies between them, these two issues are typically addressed separately. This paper presents an Integrated file Replication and consistency Maintenance mechanism (IRM). Integrated file Replication and consistency Maintenance mechanism integrates the two techniques in a systematic and harmonized manner. The security has become one of the major issues for data communication over worldwide networks. Currently many number of people using the internet. With the lack of security the data may be hacked. So in this we are introducing the routers in between the replica nodes and clients. Which protects sensitive information from unauthorized access? This routers provides security The main objective of the paper is to propose a dynamic routing with security considered using strongest algorithm, such as Blow fish algorithm which is a provide the strong security from the client to the server system. Consequently that the data which is approved by the network can't be admitted by the hackers. Without bringing up the rear data. At this point expenditure for providing The alleyway in between the client and server is fully covered with high security. It dramatically reduces overhead and yields noteworthy improvements on the competence of file replication, consistency maintenance and security maintenance approaches.**

***Keywords*— file replication, consistenancy maintenance, peer-to-peer, Router, distributed hash table, competence, Client-Server system**.

I. INTRODUCTION

In the past days, 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 supported 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[1], especially on gateway/host performance and effective network bandwidth. The 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. For 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. Therefore, we will propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages[2]. The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. 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[3]. 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. We are implementing the security algorithm such as a Blow fish algorithm which is a strongest security and fast the data processed from the client to the server. The Blow fish is provides a strongest security algorithm.

II. ROUTER MAINTENANCE

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. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing[4].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.

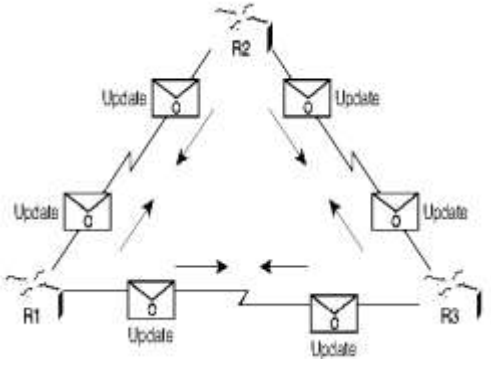

Fig1:Routers Dynamically Pass Updates

2.1 characteriristics of dynamic routing:

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

III. CRYPTOGRAPHY SYSTEM

Cryptography is the science of encrypting and decrypting written communication. It comes from the Greek word ―krypton,‖ meaning hidden, and ―graphic, meaning writing. Cryptanalysis is the process of trying to decrypt encrypted data without the key [5]. A system that provides encryption and decryption is referred to as a cryptosystem

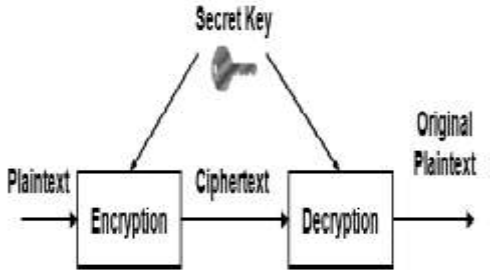

Fig2:Diagram of symmetric (single key) cryptography

1. Plain text: This is the original message or data that is fed into the algorithm as input.
2. Encryption algorithm: This algorithm performs various substitutions and transformations on the plain text.
3. Secret key: the secret key is also input the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
4. Cipher text: this is the scrambled message produced as output. It depends on the plain text and the secret key. For a given message, two different keys will produce two different cipher texts.
5. Decryption algorithm: this is essentially the encryption algorithm.

Blow fish algorithm is 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.

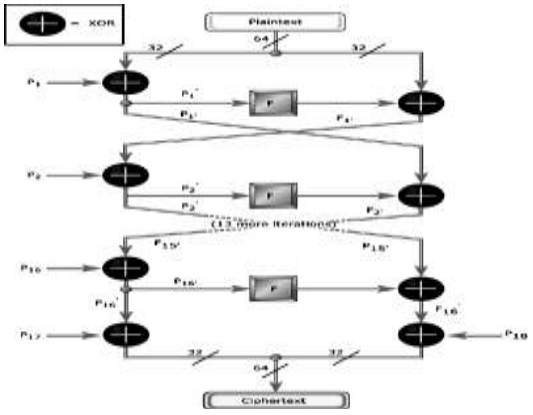

Fig:3 Blow fish algorithm

The below fig tells Festal 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 [6]. A shown in the above figure 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 summarise the procedure as follows:[7]P is an array of eighteen 32-bit integers.

- S is a two-dimensional array of 32-bit integer of dimension 4x256.
- Both arrays are initialised 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 zeros is encrypted; the results of the encryption are written back to the P and S arrays[8]. The P and S arrays are now ready for use.

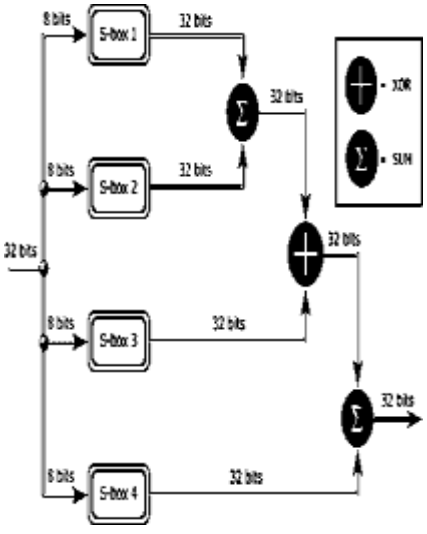

Fig4:Graphic representation of F

A. Dynamic routing with Blow fish algorithm in the Multiple Organization system

Now-a-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 Dynamic routing with Blow fish algorithm in the Multi-Organization System 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[9].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. 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[10]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. 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. A and B both are different organizations system 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.

IV. Performance Evaluation

Blow fish algorithm must be suitable for different Applications such as Bulk encryption: The algorithm should be efficient in encrypting data files[11] or a continuous data stream. Random bit generation: The algorithm should be efficient in producing single random bits. Packet encryption: The algorithm should be efficient in encrypting packet-sized data[12]. (An ATM packet has a 48- byte data field.) It should implementable in an application where successive packets may be encrypted or decrypted with different keys. Hashing:[13] The algorithm should be efficient in being converted to a one way hash function. Special hardware: The algorithm should be efficiently implementable in custom VLSI hardware[14]. Large processors: While dedicated hardware will always be used for the fastest applications, software Implementations are more common. The algorithm should be efficient on 32-bit microprocessors with 4 k byte program and data caches. Medium-size processors: The algorithm should run on microcontrollers and other medium size processors, such as the 68HC11. Small processors: It should be possible to implement the algorithm on smart cards, even inefficiently.

Table 1: Performance Comparison Of DES,AES And Blow Fish Algorithm

Algorim	Data	Time in (Sec)	AverageMB/Sec(Approx)	Performance
DES	256MB	10-11	22-23	LOW
3DES	256MB	12	12	LOW
AES	256MB	5	51.2	MEDIUM
Blow fish	256MB	3.5-4	64	HIGH

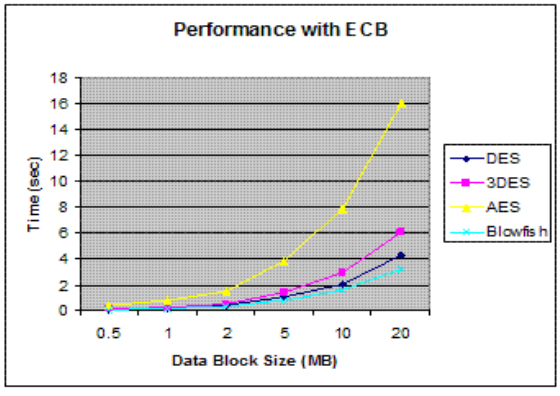

Fig4: Performance Results with ECB Mode

A. *File Replication*

File is sharing into IRM of equal size and k simultaneous connections are used. Client downloads a file from P2P at a time. Each peer sends a replication to the client[19].

B. *Security maintenance*

We are introducing a new module security maintenance. This paper proposes dynamic routing with security using a cryptographic algorithm within multiple organization system. The security has become one of the major issues for data communication over worldwide networks. The main objective of the paper is to propose a dynamic routing with security considered using strongest algorithm, such as Blow fish algorithm[15] which is a 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. In this main object of this paper is a provide strong security from many a organizations to a head of the organization, such as Banks, Colleges, Companies, Universities which is a need for strongest security for data communication from one organization to other, because any one is a hacking their data information of the organizations again have to recollect data information, so this paper main issue of a strongest security and less time for data transmission from the clients to a server.

C. *File Consistency Maintenance*

We use Hierarchy to denote the work in [16] that builds a hierarchical structure for file consistency maintenance. We compared the performance of IRM with SCOPE[17], Hierarchy[16], and Push/poll [18] methods in terms of file consistency maintenance cost and the capability to keep the fidelity of file consistency. In Hierarchy, we set the number of nodes in a cluster to 16. We assumed four types of file: highly mutable, very mutable, mutable, an immutable. The percentage of the files in each category and their update rates were (0.5 percent, 0.15 sec), (2.5 percent, 7.5 sec),(7 percent, 30 sec), and (90 percent, 100 sec). File queries were successively generated. The query interval time was randomly chosen between 1 and 500 seconds.

D. *Efficiency of File Consistency Maintenance*

File is divided into many p2p and user downloads file replication sequentially one at time. The client randomly chooses the source peer at each time slot and download the file replication from each peer in the given time slots.[21]

E. *Effectiveness of File Consistency Maintenance*

Whenever a user completes a replication from its current source peer, the user randomly selects a new source peer and connects to it to retrieve a new p2p.

Switching source peers based on chunk can reduce average time varying file download replications and updates.[21]

F. Overhead of File Consistency Maintenance

File replication is an effective method to deal with the problem of overload condition due to flash crowds or hot files. It distributes load over replica nodes and improves file query efficiency[21]. File consistency maintenance to maintain the consistency between a file and its replicas.

V. CONCLUSIONS

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. File replication needs consistency maintenance to keep the consistency between a file and its replicas, and on the other hand, the overhead of consistency maintenance is determined by the number of replicas. Connecting the two important components will greatly enhance system perform

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] The activities and labs available in the companion Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide (ISBN1-58713-204-4)http://www.traceroute.org

[5] John E. Canavan, Artech House Boston • London-Fundamentals of Network Security‖ http://www.artechhouse.

[6] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer.

[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] 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.

[9] 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.

[10] 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

[11] Lepakshi goud T ―Dynamic Routing with security using a DES algorithm‖NCETIT-2011
W. Lou and Y. Fang, ―A Multipath Routing Approach for Secure Data Delivery,‖ Proc. IEEE Military Comm. Conf. (Mil2om), 2001.

[12] W. Lou, W. Liu, and Y. Fang, ―SPREAD: Improving Network Security by Multipath Routing,‖ Proc. IEEE Military Comm. Conf. (MilCom),2003.

[13] 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

[14] Chris Mayer ―Introduction to Client/Server Systems‖ ANSA wise 24th April 1995.

[15] G. Xie, Z. Li, and Z. Li, "Efficient and Scalable Consistency Maintenance for Heterogeneous Peer-to-Peer Systems,"IEEE Trans. Parallel and Distributed Systems,vol. 19,no.12, pp. 1695-1708, Dec. 2008.

[16] X. Chen, S. Ren, H. Wang, and X. Zhang, "SCOPE: Scalable Consistency Maintenance in Structured P2P Systems," Proc. IEEE INFOCOM, 2005.

[17] Datta, M. Hauswirth, and K. Aberer, "Updates in Highly Unreliable, Replicated Peer-to-Peer Systems," Proc. 23rd Int'l Conf.Distributed Computing Systems (ICDCS), 2003.

[18] Rowstron and P. Druschel, "Storage Management and Caching in PAST, a Large-Scale, Persistent Peer-to-Peer Storage Utility,"Proc. ACM Symp. Operating Systems Principles (SOSP), 2001.

[19] Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer

[20] Donal ― Distributed system‖ Connexions IBC Plaza Houston on Aug 25, 2009