International Journal of Engineering Inventions
ISSN: 2278-7461, www.ijeijournal.com
Volume 1, Issue 2(September 2012) PP: 62-65

Providing Security for Data in Multicasting Using Encryption

M.Kiran Kumar[1], B.N.V.MadhuBabu[2], K.Nageswrarao[3]
[1]Pursuing M.Tech In Motherteresa Institute Of Science And Technology, CSE Dept, JNTUH, A.P. ,India
[2,3]Assoc.Prof In Motherteresa Institute Of Science And Technology, CSE Dept, JNTUH, A.P ,India

Abstract—In this paper we describe about providing security for data in multicasting. In multicasting multiple numbers of users share the data, from which the server sends the data to users. The data may be in general or confidential. The data is send from source to destination, in this data transformation there is a chance of malicious attack. So in order to protect the data a key is known as encryption and decryption is used .the data is encrypted before it is send to the multiple users along with decryption key Information Security has become an important issue in data communication. Encryption has come up as a solution, and plays an important role in information security system. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power and computation time.

Keywords—Encryption, multicasting, decryption, AES, RC4.

I. INTRODUCTION

For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form. Only user having access to the key can decrypt the encrypted data. Encryption is a fundamental tool for the protection of sensitive information. The purpose to use encryption is privacy (preventing disclosure or confidentiality) in communications. Encryption is a way of talking to someone while other people are listening, but such the other people cannot understand what you are saying .Encryption algorithms play a big role in providing data security against malicious attacks. In mobile devices security is very important and different types of algorithms are used to prevent malicious attack on the transmitted data. Encryption algorithm can be categorized into symmetric key (private) and asymmetric (public) key In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).Public key encryption is biased on mathematical function, computationally intensive and is not very efficient for small mobile devices .The present scenario uses encryption which includes mobile phones, passwords, smart cards and DVDs. It has permeated everyday life and is heavily used by much web application. Organization of the paper. The paper is organized as follows: In Section 2, we describe the problem of group key distribution and discuss some related solutions. In Section 3, we describe our family of key management algorithms for revocation and present sample algorithms from this family. In Section 4, we describe the key distribution process for adding users to the group. In Section 5, we present the simulation results of our algorithms and compare their performance with previous solutions. In Section 6, we describe a scenario in which users have variable requirements and show that our algorithms can adapt to such situations. In Section 7, we describe two key assignment approaches to reduce the keys stored at different users. In Section 8, we combine our algorithms with an existing solution and show its benefits. In Section 9, we conclude the paper and discuss future work. Confidential communication is a basic security requirement for modern communication systems. Solutions to this problem prevent an attacker that observes the communication between two parties from accessing the exchanged data. We address a related, but harder, problem in a scenario where the attacker is not only able to observe the communication between the parties, but can also fully compromise these parties at some time after the confidential data has been exchanged. If a protocol preserves confidentiality under such attacks, we say that it provides forward secrecy under full compromise. This is a stronger notion than forward secrecy [18], which guarantees confidentiality when participants' long-term secrets (but not their devices or passwords) are compromised. For example, a subpoena is issued and the communication parties must relinquish their devices and secrets after (e. g., e-mail) communication took place. In this scenario, the parties would like to guarantee that the authorities cannot access the exchanged information, even when given full access to devices, backups, user passwords, and keys, including all session keys stored on the devices.

Assuming public communication channels, any solution to the above problem must ensure that the communication is encrypted to prevent eavesdropping. The challenge in solving this problem is the appropriate management and deletion of the keys used to encrypt the data. Several solutions to this problem have been proposed. First, the Ephemerizer system stores the encryption keys on a physically separate, trusted server accessible by all communicating

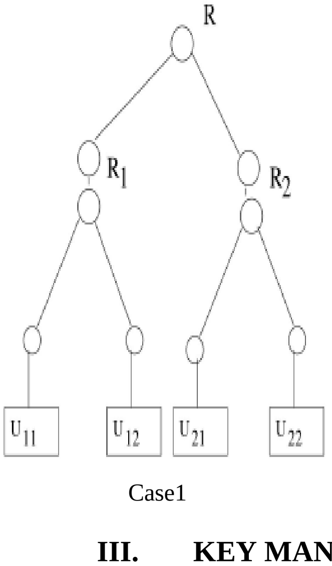
II. RELATED WORK

To reflect current group membership, the group controller also needs to change and distribute the shared keys that are known to the revoked users. There are two approaches available with the group controller for distributing the new shared keys. In the first approach, the group controller explicitly transmits the new shared keys (e.g., in [2], [3], [5]) to the current users. In our work, we adopt the second approach where the group controller and the users update the shared keys using the following technique, where kx is the old shared key, k0x is the new shared key, and f is a one-way function. Using this technique, only those current users who knew the old shared key kx will be able to get the new shared key k0x. This technique was also used in [4], [7], [13], [14], [15], [16]. However, this technique may be prone to long-term collusive attacks, as described [4], by the revoked users. To provide resistance against such attacks, the group controller adopts a policy in which the keys known to the current users are refreshed at regular intervals of time. From the above discussion, we note that the rekeying cost for the group controller to revoke multiple users is the cost of sending the new group key. We measure this cost in the number of messages sent and the encryptions performed by the group controller for distributing the new group key. Other approaches to address the problem of revoking multiple users are proposed in [17] the group controller maintains a logical hierarchy of keys that are shared by different subsets of the users. To revoke multiple users, the group controller aggregates all the necessary key updates to be performed and processes them in a single step. However, the group controller interrupts the group communication until all the necessary key updates are performed, and then, distributes the new group key to restore group communication. This interruption to group communication is undesirable for real-time and multimedia applications. In [18], to handle multiple group membership changes, the group controller performs periodic rekeying , i.e., instead of rekeying whenever group membership changes, the group controller performs rekeying only at the end of selected time intervals. From the above discussion, we note that the rekeying cost for the group controller to revoke multiple users is the cost of sending the new group key. We measure this cost in the number of messages sent and the encryptions performed by the group controller for distributing the new group key

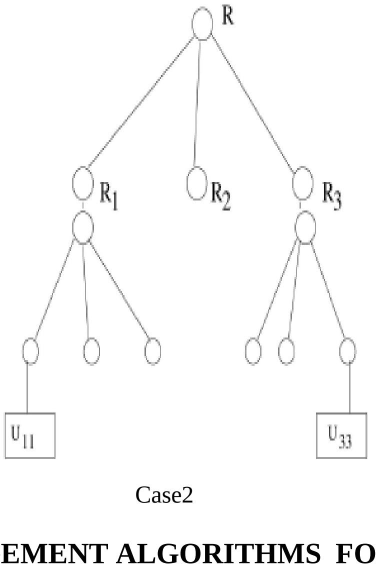
Theorem: In the basic structure, when one or more users are revoked, the group controller can distribute the new group key securely to the remaining users using at most any one encrypted transmission.

Proof: We consider three possible cases of user revocation from the basic structure.
Case 1: When no users are revoked, the group controller sends the new group key using the current group key that is known to all the users. Although this trivial case is not important for the basic scheme, it is important for the hierarchical algorithm we describe in later sections.
Case 2: When m < K, users are revoked from the group and the group controller needs to distribute the new group key to the remaining K -m users. The group controller uses the shared key k_{K-m}associated with the

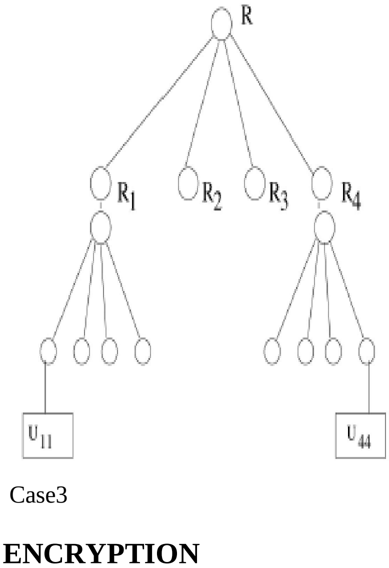
remaining subset of K _m users to send the new group key. Thus, the group controller transmits$k_{K-m}\{k'_g\}$. As the revoked users do not know k_{K-m}, only the current users will be able to decrypt this message.
Case 3: All users are revoked from the group. The group controller does not need to distribute the new group key, and thus, does not send any messages. We note that once the new group key is distributed, the current users update the necessary shared keys using the one-way function technique we described in Section 2. However, the basic structure requires the group controller and the users to store a large number of keys, which is not practical if the group is large. In the next Section, we present our hierarchical algorithm to reduce the number of keys stored at the group controller and the users. Our hierarchical algorithm preserves some attractive communication properties of the basic structure while reducing the storage requirement for the shared keys.



Case1



Case2



Case3

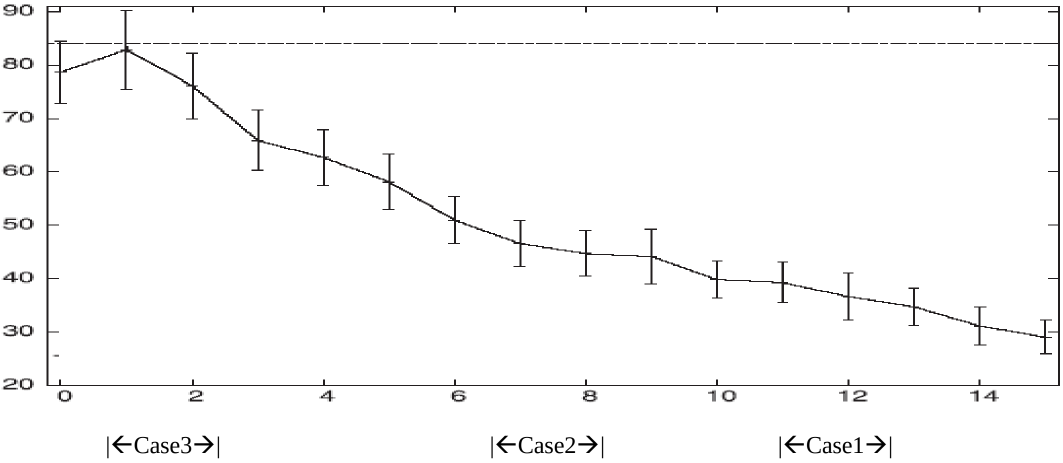
III. KEY MANAGEMENT ALGORITHMS FOR ENCRYPTION

AES: The Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. It has a variable key length of 128,192 or 256 bits. It encrypts data blocks of 128 bits in 10, 12, 14 rounds depending on key size. AES encryption is fast and flexible in block ciphers. It can be implemented on various platforms. AES can be operated in different modes of operation like ECB, CBC, CFB OFB, and CTR. In certain modes of operation they work as stream cipher.

RC4: RC4 is a stream cipher designed in 1987 by Ron Rivest. It is officially termed as "Rivest Cipher 4". Stream ciphers are more efficient for real time processing. It is a variable key size stream cipher with byte oriented operations.This algorithm is based on the use of a random permutation. According to the various analysis,the period of the cipher is greater than 10100.Eight to sixteen machine operations are required per output byte and the cipher run very quickly in software. The algorithm is simple, fast and easy to explain. It can be efficiently implemented in both software and hardware.

IV. RESULTS AND ANALYSIS

We compare the performance of our algorithms with the Algorithms, the group controller associates a set of keys with the nodes of a rooted tree and the users with the leaves of the tree. Each user knows the keys associated with the nodes on the path from itself to the root. To revoke a user, the group controller recursively distributes the changed keys at the higher levels in the key tree using the changed keys at the lower levels. To revoke multiple users the group controller processes all the key updates in a single step.This reduces the cost of changing a key multiple times.



V. CONCLUSION

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 addressed the problem of data confidentiality in scenarios where attackers can observe the communication between principals and can also fully compromise the principals after the data has been exchanged, thereby revealing the entire state of the principals' devices. In this paper, we presented a family of algorithms that provide trade-off between the number of keys maintained by the users and the time required for rekeying due to the revocation of multiple users. Encryption algorithm play an important role in communication security where encryption Time, Memory usages output byte and battery power are the major issue of concern. The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Our algorithms are also suited for overlay multicast applications. In overlay multicast, the end nodes perform the processing and forwarding of multicast data without using IP multicast support. The solutions provide users with full control over their data privacy. Our future work will include experiments on image and audio data and focus will be to improve encryption time and less memory usage.

ACKNOWLEDGMENT

The great full thanks to all author's because of working of this paper presentation, References also used for developing this IEEE transactions

REFERENCES

1. DiaasalamaAbdElminaam, HatemMohamadAbdual Kader,Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.
2. Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms",
3. International Arab Journal of e-technology, vol 2,no.1,January 2011.
4. Lepakshi goud T ―Dynamic Routing with security using a DES algorithm‖ NCETIT-2011 .
5. Donal ― Distributed system‖ Connexions IBC Plaza Houston on Aug 25, 2009 .
6. G. Manikandan, R. Manikandan, G Sundarganesh, "A New approach for generating Strong Key in RivestCipher4 Algorithm", Journal of Theoretical and Applied Information Technology, 2011,pp.113-119.
7. N.Sairam, G.Manikandan, G. Krishnan, "A Novel Approach for Data Security Enhancement using Multi Level Encryption Scheme", International Journal of Computer Science and Information Technologies, Vol.2(1),2011, pp.469-473.
8. Deguang Le, Jinyi Chang, Xingdou Gou, Ankang Zhang, Conglan Lu, "Parallel AES Algorithm for Fast Data Encryption on GPU", 2nd International Conference on Computer Engineering and Technology, Vol.6, ,2010, pp.v6-1-v6-6.

9. G.Manikandan, R.Manikandan,P. Rajendiran, G.Krishnan,G.SundarGanesh, An Integrated Block and Stream Cipher Approach for Key Enhancement , Journal of Theoretical and applied information Technology, 2011, Vol 28 (2), 83-87.
10. G. Manikandan, M.Kamarasan,P.Rajendiran, R.Manikandan, A Hybrid Approach for Security Enhancement by modified Crypto- Stegno scheme, European Journal of Scientific Research, vol.60(2) , 2011, 224-230.
11. G.Manikandan, N.Sairam, M.Kamarasan, A New Approach For Improving Data Security Using Iterative Blowfish Algorithm in Journal of Applied Sciences, Engineering and Technology,Vol 4(6) , 2012,603-607
12. G.Manikandan, N.Sairam, M.Kamarasan, A Hybrid Approach For Security Enhancement by Compressed Crypto-Stegno Scheme in Research Journal of Applied Sciences, Engineering and Technology,Vol 4(6) ,2012, 608-614.
13. B.Karthikeyan, V.Vaithiyanathan, B. Thamotharan, M.Gomathymeenakshi and S.Sruthi, LSB Replacement Stegnography in an image Using Psudorandomised Key Generation. Research Journal of Applied Sciences, Engineering and Technology, 4(5), 2012, 491-494.
14. Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir .M and Al-Nabhani.Y, "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal of Computing, Volume 2, Issue 3, March2010, ISSN 2151-9617, pp.152-157 .
15. Salama Diaa , Kader Hatem Abdual , and Hadhoud Mohiy , "Studying the Effects of Most Common Encryption Algorithms" International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011, pp.1-10.
16. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed,"Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security,Vol.10, No.3,pp.213- 219, May 2010.
17. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms" International Journal of Computer Theory And Engineering, Vol.1,No.3,pp.325-333 August 2009.
18. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, pp.78- 87, Sept. 2010.

.