iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2028

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

A Survey on Secure Information Transfer with Authentication Service

M. Elakkiyathasan[1], T. Kishore Kumar[2], G. Madhan[3], Ms. G.Gowri[4]
[1, 2, 3] *U.G. students, Computer Science and Engineering, S.A. Engineering College, Chennai*
[4] *Assistant professor, Computer Science and Engineering, S.A. Engineering College, Chennai*

Abstract: ***In order to realize secure information sharing, it is common to encrypt information, using a common key called 'Group Key' among group members. However, in the case of existing technologies, there is a concern that leakage of information occurs because contents of communications are preserved at the server, and also because the server administrator possesses the group key. Securing the information with the encryption technique is weaker in the existing technologies and to enhance the security of the information, we propose this method of encryption. Encryption will be stronger by the way where encryption key between the administrator and each member will be differed. Thus, the information will be more secured.***
Key points: Group key, administrator, users, authentication, information, security, IGMP and KDC.

I. INTRODUCTION

Secure group communication plays a vital role for applications like scientific discussions, project management, teleconferencing, etc. Secure group communication involves confidential message delivery between the administrator and the authorized users. Applications like scientific discussion and project management may lead to a scenario in which it is necessary to set up multiple secure groups simultaneously and few members may be part of several secure groups. Therefore, each independent group should have its own group key. The shared key may later be used to achieve some cryptographic goals like multicast message confidentiality or multicast data integrity, such as interactive chatting, etc. Although the improved protocol uses a signature scheme to achieve authentication, we find that it is still insecure. So, we propose a method to provide more security to the information by the way of encryption between the administrator and each authorized user. IP multicast (hereinafter multicast) is an efficient group communication protocol to deliver multicast content from a single source to multiple users. This communication technology uses IGMP (Internet Group Management Protocol) for group membership that allows members to join the group and receive content freely. As a result, open group membership by IGMP leads to eavesdropping. In order to avoid this threat, group key management has been proposed. Group key is a key shared by all group members and the sender for encrypting data by the sender and decrypting transmitted data by the group members.

II. RELATED WORKS

A. *R. Aparna [1] proposed Key Management Scheme for Multiple Simultaneous Secure Group Communication*

In various applications such as project management, teleconferencing requires secured group communication for the transmission of secured messages or files. In such cases multiple secure groups are in need to be created. Therefore there may be overlapping of members. To avoid this each group should have their own group keys. Maintaining these many group keys is a tedious process and so a key management scheme is been proposed in this paper for managing the multiple groups. In this paper two approaches are been used for managing the keys and those approaches are key based and secret share-based approaches. This mechanism provides authentication for multiple groups also membership changing events is handled in this mechanism. In this approach a group key is been used which is considered as the secret key through which the users who has the group key can only recover the message after decrypting it. A communication known as backward access control and forward access control which are been used to handle the new members entry and new members exit. In this key management scheme initially the group is been set up and then only the group key is been computed. Thus this paper provides the authentication for the group communication.

B. *Armando Faz-Hernandez [2]proposed a Faster Software Implementation of the Super singular Isogeny Diffie -Hellman Key Exchange Protocol*

This paper is based on the new research on isogeny based cryptography. In super singular isogeny diffie-Hellman key exchange mechanism the two entities share a secured key on an agreement. In this approach the secret key is determined by finding the j invariant of two isomorphic super singular elliptic circles formed by the communication between the two entities. In this mechanism

a novel algorithm for computing one entity's variable point is proposed. And the algorithm is Montgomery algorithm which is also known as left-to-right algorithm. The various optimizations on targeting the super singular isogeny exchange protocol is been done in this paper. The finite field and the elliptic curve arithmetic key layers are been mainly optimized. Also a formula for computing the elliptic curve point tripling is been proposed in this paper. Thus this ensures the faster implementation of the super singular isogeny Diffie-Hellman key exchange protocol.

C. Mike Burmester [3]proposed a Secure and Efficient Conference Key Distribution System

The communication over the insecure channels can be done only if the secret keys are been distributed securely. Unless and until the secret keys are been distributed securely the whole system is vulnerable even though the encryption algorithm is been used. Many systems are been proposed based on the research on the security and the efficiency of the communication. The most commonly used system is the Diffie- Hellman key exchange system for distributing the secret keys. Recently many conference key distribution systems are been proposed. A common key distribution system is been proposed by Ingemarsson, Tang and Wong for which the common key is the symmetric function. Even though it has many advantageous features it is possible that the information shared can be heard by the passive eaves dropper. And it uses a cyclic function which prevents the information from the passive eaves dropper. The computation of the common key is independent of the number of conference users. In this paper conference key distribution is been used to provide security against the passive eaves dropper. There is an authentication scheme for authenticating the messages. Thus this approach provides a secure and efficient conference key distribution system for the efficient transmission of the messages.

D. N. Vimala [4] proposed Efficient Group Key Management Protocol for Region Based MANETs

In this paper for region based MANET a simple and efficient group key management scheme is been proposed. Considering the security of the transmission of the messages in the group communication the key management is a complex process. The various categories of the group key management are centralized, decentralized and distributed. These key management protocols provide authentication, integrity and confidentiality. A simple and efficient group key (SERGK) management scheme is proposed for the region based MANET. A collection of multiple independent nodes is the adhoc network in which the nodes communicate with each other by wireless multihop. The intermediary between the nodes of communication is the Trusted Third Party systems. The appropriate solution to provide the transmission of messages with authentication, security and data integrity is the key management system proposal. The basic idea behind the SERGK is to build a physical multicast tree for the MANET for efficiency. Hence the users can share the intermediary key among themselves rapidly. Thus this paper provides an simple and efficient method which divides the groups into sub groups based on the DE generalized key management scheme. Thus this paper provides an efficient protocol for the group communication.

E. Amjadsaeed khan [5] opportunistic Relaying And Random Linear Network Coding for Secure And Reliable Communication

Opportunistic relaying helps to achieve full diversity gain and Random linear network coding (RLNC) reduces delay and energy consumption. This paper speaks about the multi-relay network where the relay nodes use the RLNC for encoding the confidential data and also to transmit the encoded packets to the destination. This framework which is the combination of random linear network coding with application layer and physical layer with or without jamming was developed to address the problem of vulnerability of wireless communication network against eavesdropping attacks. Four relay sel4ction protocols are considered and to measure the amount of information leakage to the eavesdropper, intercept probability is proposed. The selection of the relay and jammer can be traided for security. The introduction of the direct communication from the source to the destination cannot be heard by the eavesdropper.

F. Melisa Hakyvahabzadeh [6] an effIcient Group key Management Using Code for key Calculation for Simultaneous join/leave: ckcs

An efficient group key management control protocol is been proposed in this system. CKCS(Code for Key Calculation for Simultaneous Join/Leave) in the multicast communication. This mechanism is based on the logical key hierarchy approach. In this protocol the server automatically sends the group key to the members who are newly joining to the group. Then the one way hash functions and the necessary keys are been calculated by the new members and the current members of the group. In this approach the computation overhead is been reduced and also the size of the messages are also reduced. The multicast messages can be delivered to the users using the efficient protocol IP multicast and IGMP(Internet Group Management Protocol). In order to overcome eaves dropping in open group membership of IGMP the key management scheme is been proposed. The rekeying is also used to handle new member entry and the exit of existing members. In single join/leave only one user's request is been replied by the server. But in simultaneous join/leave the server

should reply for the multiple responses. Thus in this paper with the proposal of the efficient group key management algorithm CKCS the message size is been reduced in the unicast communication.

G. Nik Unger [7]SoK: Secure Messaging

Many of the messaging tools that are been used on the internet do not provide the end to end security. In this paper a frame work has been evaluated for their security and the way in which they adopt the properties. The three key challenges are been identified and then the design for those challenges are been proposed in this paper. The challenges are trust establishment, conversation security, transport privacy. The trust establishment approach is designed in such a way that strong security is been ensured. Transport privacy approach is been designed in such a way that the payment of some penalties are been avoided. And the conversation security approach is been achieved through not involving the users in most of the two part communication. The major contributions of this paper are to establish secure and privacy message transmission, secured message transmission for both academic works and wild projects, a comparative analysis of these approaches, and finally to identify and discuss the current research challenges. The secure message system specifications can be done in three categories such as chat protocols, wire protocols and tools. The conversation security deals with how the messages are been encrypted. The transport privacy layer deals with how the messages are been exchanged within the sender and the receiver with an objective of hiding the message metadata. Thus this paper provides a systemized design of the message transferring with trust establishment, conversation security, and transport security. These schemes are been chosen independently to get a secured message transmission system. There are many solutions provided in this paper for many of the uncovered problems in the world which would be the real world advantages.

H. Pejman Dashtinejad [8]Security System for Mobile Messaging Applications

In this paper an end to end encryption(E2EE) approach is been designed to provide a secured way of message transmission. Since the instant message applications are the tending applications of the smart phones, there should be a secured way of message transmission. This end to end encryption design provides privacy, confidentiality and integrity. The main objective of this paper is to design the secured system for the mobile messaging applications. These mobile messaging applications provide the many advanced built in features whereas it lacks to provide the secured communication. The main aim of this paper is to design a chat application which is much secured and protects the user's confidentiality and privacy. Also it provides solutions for the various security challenges faced by the current mobile messaging applications. The cryptography algorithms are been discussed to ensure the confidentiality of the users. The two categories of the algorithms are symmetric key cryptography and asymmetric key cryptography. In the symmetric key cryptography both the sender and the receiver uses a shared key to encrypt and decrypt the messages. But in asymmetric key cryptography two separate keys are been used for the encryption and decryption. Authentication is achieved through one time passwords (OTP) and certificate based authority (CBA). And integrity is achieved through hashing mechanism. Thus this paper provides an architectural design for the secured mobile messaging application system which ensures integrity, confidentiality and privacy.

I. B.R. Purushothama [9]Group Key Management Scheme for Simultaneous Multiple Groups with Overlapped Membership

The multiple groups are been managed by the key management scheme. In this paper a key management scheme is been proposed for managing the multiple groups. When same people of one group is a member of another group involved in a project then how to ensure the secured way of communication within the group and also with the other groups. To overcome this problem the key management scheme is been proposed with overlapping membership. In this paper key user tree approach is been used. This scheme ensures three things such as handling of multiple groups, groups can communicate within themselves in a secured way, groups can communicate with the other groups in a secured way. In this approach join/leave protocols are been used for storing, key changes and encryption. This approach provides reduction of rekeying cost when compared with the older rekeying techniques. For the secured group communication forward access control and backward access control are been used. The Lagrange form of interpolation polynomial is been used to find the membership overlapping in the groups. To manage the multiple groups a key tree structure is been used which is been constructed by the key distribution center (KDC). The key user tree (KUT) is based on the logical key tree structure (LKT). The various join group protocols for the parents and the non- parents are been discussed. Similarly the various leave protocols for the parents and the non-parents are been discussed. This paper provides a new key management scheme for the simultaneous multiple groups using the key user tree (KUT) approach.

J. Pratima Adusumilli [10]DGKD: Distributed Group Key Distribution with Authentication Capability

To maintain a secured group communication management of the group key is an essential thing. But at the same time it is a complex process too. The existing protocols or mechanism for maintaining the group keys requires the existence of central trusted authorities such

as group holders, group controllers and so on. A new class of group key management is been proposed in this paper named DGKM (Distributed group key distribution) which provides the solution for the above mentioned problems. This DKGM is much better than the existing GKM in scalability, robustness and also efficiency. This DGKM does not require any of the central trusted authorities. This protocol construct a tree structure for the members present in the group and perform the rekeying operation in two rounds. This protocol also allows authentication. Hence all these above properties make this new protocol an efficient, robustness and scalable one. This DGKM protocol consists of three mechanisms to implement and distribute the group keys and they are the intermediate node keys are considered as the secret keys, leaf nodes are the public keys, the rekeying and the key generation is been done by the joining or the leaving member of the group, the new keys are been distributed to the new members of the group in a parallel manner. By doing this all the members of the groups are considered equally so that there won't be any dependence on the single entity. For this reason this proposed protocol is been considered as the robust one. The join, multiple join, leave, multiple leave protocols are been designed in this approach. Thus this DKGM protocol provides secured group communication with authentication by using the above algorithms.

K. Punam V. Maitri [11] Secure File storage in Cloud computing using Hybrid Cryptography Algorithm

Cloud computing is the rapid growing technology which is been used to store the huge amount of data where we can retrieve the required data whenever required on paying some amount or at free of cost. But there are many issues to be faced when storing the data on the cloud. Hence data security should be achieved while storing the data on the cloud. Cryptography and steganography are the two main mechanisms which are been used to provide the data security. In this paper using symmetric key cryptography algorithm and steganography data security to data in the cloud is been achieved. Various algorithms such as blowfish, AES algorithms are been used to provide security for the data block wise. To achieve information key security the LSB steganography technique is been used. Using the multithreading techniques the divided files are been encrypted simultaneously. The files are been divided into eight parts. And for the file decryption process, the reverse process of the file encryption is been followed. Converting the file into unreadable format is the main objective of the cryptography technique. So that only the authorized people can only access the data. The various cryptography algorithms are been used to provide high level security. Steganography hides the data existence and so only the known users can access the data required which is the high security for the users data stored on the cloud. Thus in future this paper has been suggested to provide hybridization of the public key cryptography algorithms.

L. Hugh Harney [12]Group based cooperation on symmetric key generation for wireless body area networks

The wireless body area networks require the efficient security approaches for the resources. Thus additional sensing hardware requirements are been used in every approaches which is a complex process. In this paper a physical layer approach is been proposed to remove the hardware requirements. A practical group solution is been provided to increase high efficient key generation. Several group models are also been proposed with the specific protocol design. The received signal strength indicator (RSSI) is been measured at receiving side. This data has remarkable similarity on both sides. The big complexity is that RSSI key based generation because of the reduced communication overhead there is a possibility of information leaking. This paper proposed a physical layer characteristic. These characteristics are proposed for the security approach and also to improve the generation of the symmetric key generation by loading the major tasks to the senior assistants. This proposed system gives a speed up key generation process. This method of approach does not require any extra or special hardware requirements. Therefore the multiple data density can be achieved which leads to the high key generation rate. This proposed system works smoothly with the node authentication methods. To build a trusted relationship between the newly joined node and the wireless body area networks, the node authentication is the first step. The speed up process of the key generation process benefits the resource constrained wireless body sensors. Thus this paper provides a security based approach for the key generation method.

M. Manman Geng [13]AGKA

Authenticated Group Key Agreement protocol uses only two communication round and for each run only four computations is involved for every participant. This protocol uses the strongest security model, Signature for ensuring authentication. Thus this protocol ensures Key authentication, security for session key, forward security, security for compromise impersonation and temporary information security. First the secure certificate less signature based scheme is introduced for the message with private key and public key to compute the signature. Now the two rounds of group key agreement protocol is CL-AGKA is done after the signature scheme. Thus this protocol achieves the two security attributes as the certificate less signature scheme mentions about the two types of adversaries namely, the type I adversary who doesn't have the access to the master key but uses arbitrary values of its own choice and the type II adversary also doesn't have the access to master key and also cannot replace the entities of public keys.

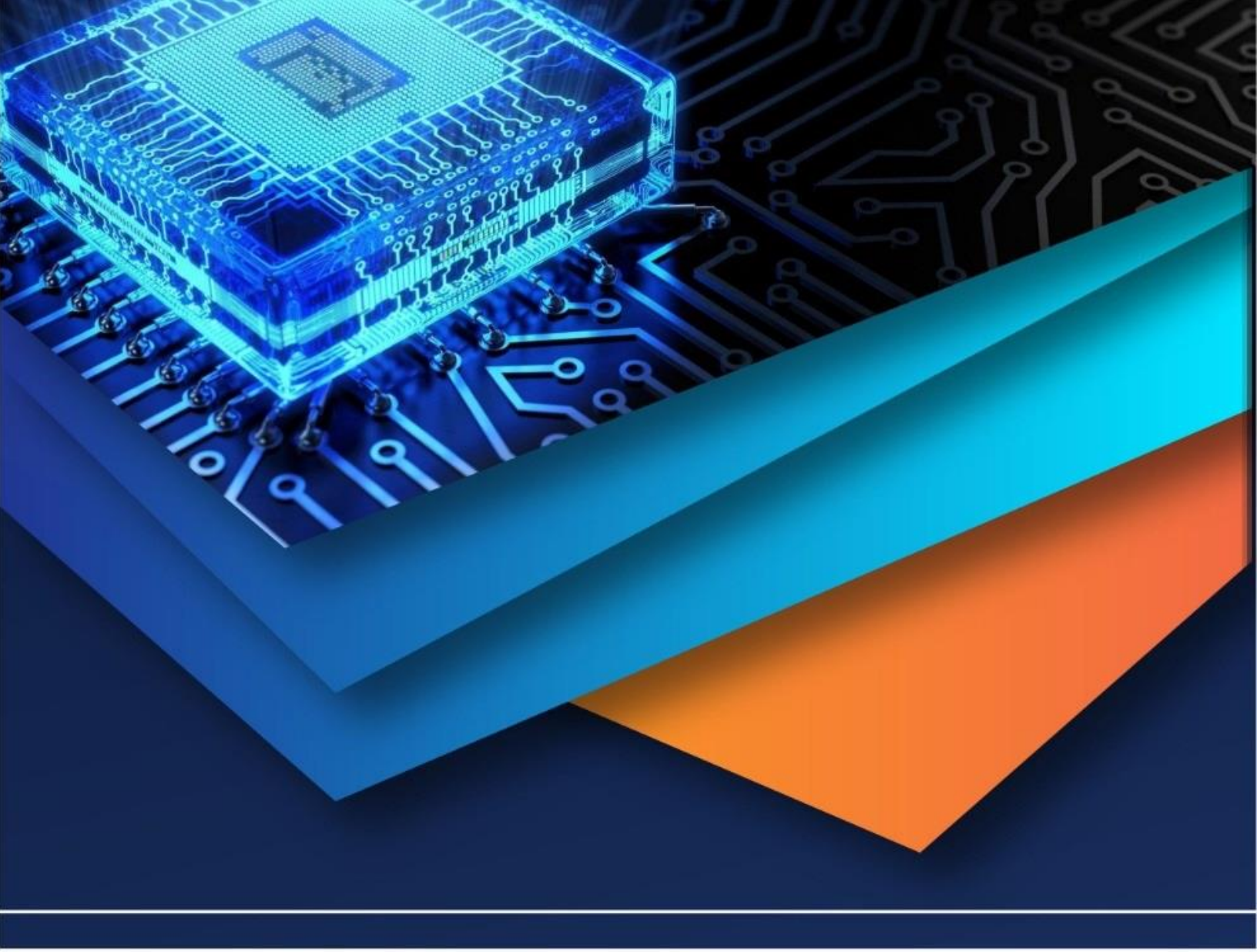
Thus the Authenticated Group Agreement protocol achieves the all the requirements needed for the group agreement protocols. The protocol is also efficient because it requires only two communication round and only four computations for each participant. This high efficiency makes it possible to get used in various applications like conference key establishment, multicast and adhoc network group security.

III. CONCLUSION

In existing group communication systems, the problem was that malicious key server administrators could read communication contents because the group key remains in the key server. Accordingly, in this Paper, we proposed a method of sharing two types of random numbers of different generation origins through different distribution routes, and of using these two types of random numbers to create a group key. Based on this method, secure group communication is guaranteed. We also indicated that our proposed method satisfies key management requirements. Hereafter, we will plan to implement our proposed method to actual devices and conduct performance evaluations.

REFERENCES

[1] R. Aparna, Dept. of Computer Science and Engg., Siddaganga Institute of Technology, Tumkur, Karnataka, India and B.B. Amberker, Dept. of Computer Science and Engg., National Institute of Technology, Warangal, Andhra Pradesh, India on "Key Management Scheme for Multiple Simuktaneous Secure Group Communication"
[2] Armando Faz-Hernandez, Member, IEEE, Julio Lopez, Member, IEEE, Eduardo Ochoa-Jimenez, Member, IEEE, and Francisco Rodriguez-Henriquez, Member, IEEE on "A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol".
[3] Mike Burmester, Dept. of Mathematics, Royal Holloway – University of London, Egham, Surrey, TW20 OEX, U.K. and YvoDesmedt, Dept of EE&CS, University of Wisconsin – Milwaukee, P.O. Box 784, WI 53201 Milwaukee, U.S.A. on "A secure and Efficient Conference Key Distribution System".
[4] N.Vimala, B,Jayaram, Dr.R.Balasubramanian on "Efficient Group Key Management Protocol on Region Based MANETs"
[5] AmjadSaeed Khan, Student Member, IEEE and IoannisChatzigeorgiou, Senior Member, IEEE on "Opportunistic Relaying and Random Linear Network Coding for Secure and Reliable Communication".
[6] Melisa Hakyvahabzadeh, ElinaEidkhani, S. AnahitaMortazavi, AlirezaNemaneyPour"An Efficient Group Key Management Using Code For Key Calculation For Simultaneous Join/Leave: CKCS".
[7] Nik Unger, SergejDechand, Joseph Bonneau, SaschaFahl, Henning Perl, Ian Goldberg, Mathew Smith on "SoK: Secure Messaging".
[8] PejmanDashtinejad on "Security System for Mobile Messaging Applications".
[9] B.R. Purushothama and B.B. Amberker, Computer Science and Engineering, National Institute of Technology, Warangal, India on "Group Key Management Scheme for Simulataneous Multiple Groups with Overlapped Membership".
[10] PratimaAdusumilli, XukaiZou, Byrav Ramamurthy on "DGKD: Distributed Group Key Distribution with Authentication Capability".
[11] Punam V. Maitri and ArunaVerma, Department of Computer Engineering, Dhole Patil College of Engineering, Pune, India on "Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm".
[12] Hugh Harney on "Group Secure Association Key Management Protocol (GSAKMP)"
[13] ManmanGeng, Futai Zhang, MengGao, College of Computer Science and Technology, Nanjing Normal University, Jiangsu Information Security and Confidentiality Technology Engineering Research Center, Nanjing, P.R. China on "A Secure Certificateless Authenticated Group Key Agreement Protocol".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY