ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

Computation Efficient Multicast Key Distribution

AkulaGopi[1],Dr.P.Chiranjeevi[2]
PG Student[1], Professor&HOD[2]
Department of Master of Computer Applications
Amrita Sai Institute of Science and Technology
Paritala,NTR(Dist),Andhra Pradesh
gopiakula630@gmail.com

ABSTRACT

Efficient key distribution is an important problem for secure group communications. In many applications, multicast is an efficient means of distributing data in terms of resources usage. The privacy of a multicast communication session is usually ensured using symmetric encryption. All the designated receivers or members in a multicast group share a session encryption key. In many applications, the multicast group membership changes dynamically.Thus, session keys shall change dynamically to ensure both forward secrecy and backward secrecy of multicast sessions. Each session thus needs a new key that is only known to the current session members i.e., session keys need to be dynamically distributed to authorized session members(Arial size 10 normal)

I.INTRODUCTION

The Computation-Efficient Multicast Key Distribution for Large and Dynamic Multicast Groups provides an efficient way of Group key Distribution in terms of Scalability and Authenticity between the Sub group members and to other group members in the network. The Existing system have the drawbacks such as the Group Controller takes all responsibilities of key generation, re keys generation, message transmission to its sub group members and also to any other group controllers. So lot of Storage and computation complexity occurs.

The sub group's members are not able to send information's to any other subgroup at the time of re keying process. So performance of the sub group degrades at that time. The re keying process is done every time once a communication is completed between the users in the same group or to any other group members.

II.RELATED WORK

Existing System :The communication complexity is usually ensured by the number of data bits that need to be transmitted from the GC to group members to convey information of session keys, whereas the storage complexity is measured by the number of data bits that the GC and group members need to store to obtain session keys. Another similarly important but usually under noticed, if not ignored, factor is the computation complexity, which can be measured by the number of computation operations (or the computation time on a given computing platform) that the GC and group members need to distribute and extract session keys. Hereafter, the problem of how resources can effectively be used to distribute session keys is referred to as the group key distribution problem

Draw Back:-The group controller maintains whole group member's information, so increase the storage complexity.The group members are not able to communicate with any other groups during the re keying process.The Group controller takes all responsibilities for the group such as key generation, re keying process and message transfer to any other groups

Proposed System: The complexity of the rekeying operation is asymmetric between a new member’s join and an old member’s leave. When a new member joins, the GC can easily multicast the new session key encrypted by the current session key to all the current members, followed by a unicast to the new member to send the new session key encrypted by a predetermined encryption key shared between the GC and the new member. Thus, join is easy, with low communication and computation cost. However, when an old member leaves, the current session key cannot be used to convey the new session key information securely, since it is also known to the old member. Thus, hereafter, we will focus on the rekeying operation for a single member leave. The same idea can easily be extended to other rekeying operations such as batch rekeying.

III.AUTHENTICATION

This module performs authentication of group members. Each member must contact GC to get registered with the group and must obtain a private key to communicate with GC

IV.RESULTS

We have presented a dynamic multicast key distribution scheme using MDS codes. The computation complexity of key distribution is greatly reduced by employing only erasure decoding of MDS codes instead of more expensive encryption and decryption computations. Easily combined with key trees or other re keying protocols that need encryption and decryption operations, this scheme provides much lower computation complexity while maintaining low and balanced communication complexity and storage complexity for dynamic group key distribution. This scheme is thus

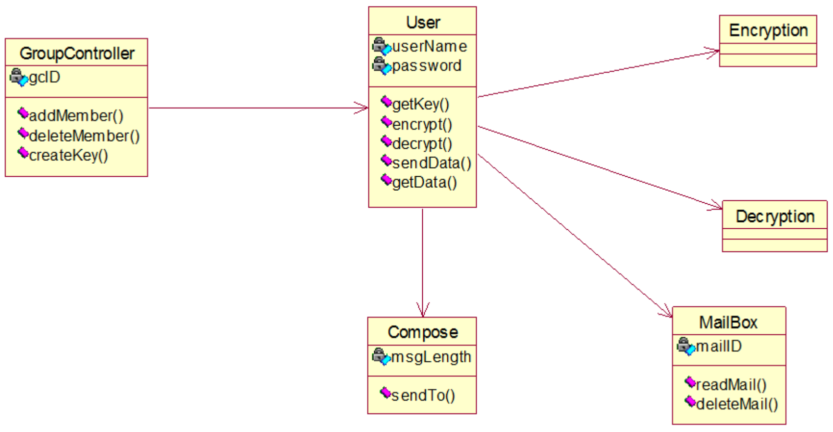
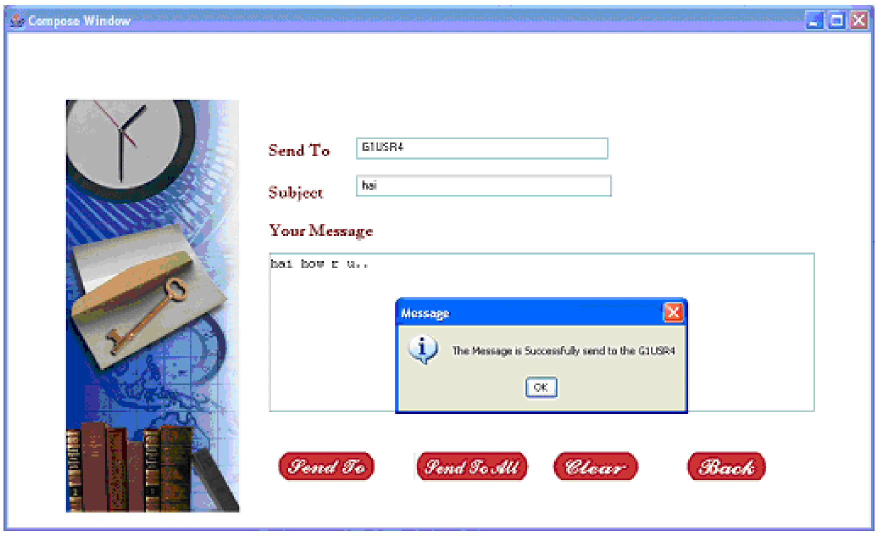


Figure 1 : Shows the Class Diagram

V.RESULT



Send To: G1USR4
Subject: hai
Your Message: hai how r u..

The Message is Successfully send to the G1USR4

VI.CONCLUSIONS

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

VII.DISCUSSIONS

How does the API support all these kinds of programs? It does so with packages of software components that provide a wide range of functionality. Every full implementation of the Java platform gives you the following features.

REFERENCES :

[1] Dr.P.Chiranjeevi, Department of CSE, for their steadfast support, direction, and use full advice. which played a crucial role in project and were essential in the creation of this thesis.