A Multi-Server approach for Generic Group Key Management in Multicast Group Communication

[1]P.Gayathri, [2]M.Arun
[1]PG Student, [2]Assistant Professor
Department of Computer Science and Engineering
Mepco Schlenk Engineering College
Sivakasi, India
[1]gayathri1492@gmail.com,[2]marun@mepcoeng.ac.in

Abstract : Group Key Management is one of the prominent area when dealing with group communication. And also it is more important to be considered when the leave and join of users in the group is dynamic. The number of users in a multicast group tends to fluctuate due to frequent user join and leave. And also due to enormous increase in the number of users the system may face scalability issues. In this paper a Master Key Management algorithm is proposed for the purpose of managing the keys within the system and a multi-server approach is proposed for balancing the load in each server and thus enhancing efficient group communication by reducing the network bandwidth. The proposed system generates a master key using the master key management algorithm and then it encrypts the key using Advanced AES algorithm. The encrypted key is distributed to the server and all the users in the group by the group controller. This encrypted key is further used for all the multicast communication within the group.