CHAPTER 3

SYSTEM ARCHITECTURE

The architecture of the system proposed in this research work for centralized multicast key management and distribution scheme used in wired networks is illustrated in Figure 3.1. This architecture consists of six components namely user interface, user database, group center, group center database, media server and media server database. The user interface module is responsible for user interactions, key updation and descrambling operations. The user database stores the user details which are used by the user interface for authentication and key updation. The group center has different modules such as user name and password generation/verification module, key generation and distribution module, group management module, rekeying module and key encoding module. The group center database is responsible for storing key and user related information. The media server is responsible for adding or deleting the multimedia data, data scrambling and multicasting it to the group of registered users. The media server database is responsible for storing the subgroup key, group key and media information.

3.1 USER INTERFACE

The user interface is responsible for providing an effective user interaction facility for the multicast communication. It has five modules namely registration module, login module, user administration module, key recovery manager and data descrambling module.
The registration module provides a menu to the user for collecting the user profile information. In the registration process, new users are asked to provide their details for completing the registration process and they will get a
unique user id, user name and password. The user name and password are used for login process and also for further communications. The user administration module handles users join and leave operations. This module allows a new user to join into an existing multicast group or new group and an existing user to leave from the existing multicast group. The key recovery manager is responsible for decoding the key received in encoded format from group center. It also performs key updating operation. The data descrambling module is responsible for decrypting or descrambling the encrypted multimedia data in order to view the media data.

3.2 USER DATABASE

The user database is responsible for storing and retrieving the user name, password and keying information for all users. This is managed by the user interface module. This database is also responsible for storing Private Key (PK), Sub Group Key (SGK) and Group Key (GK).

3.3 GROUP CENTER

The group center is responsible for generating, managing and distributing the keys to the users and media server in a secure way. It has five modules. The user name and password generation/verification module is used for authentication purpose in the group center side. The key generation and distribution module is responsible for generating and distributing secret or private key, SGK and GK randomly and uniformly in coordination with the media server. One of the main functions of this module is to generate the keys to the users and media server for performing secure multicast communication. For distribution, this module gets the key from the key generation sub module, key encoding module and distributes it to the authenticated users. The key distribution module sends a PK as a unicast message when a new user log on to the system. In addition, this module sends a multicast message
to the members of the group when SGK or GK is updated. The group management module is used to get the list of available multimedia data from media server. The group management module also forms groups for multicast communication based on the requests provided by the user interface. The rekeying module performs both single rekeying and batch rekeying operations.

The rekeying module consists of two sub modules called as single rekeying sub module and batch rekeying sub module. The rekeying module is mainly used for updating the keys when there is a change in the group memberships. Whenever a single user joins or leaves to/from the multicast group, the single rekeying sub module is invoked in order to update the keys. If a group of users joins or leaves from a multicast group then the batch rekeying sub module is invoked for updating the keys. This module gets the key related information from group center database module and sends the rekeyed message as output to key encoding module.

The key encoding module uses two processes namely pseudo tree construction and encoding stopping set construction for performing encoding operations. Pseudo tree is an extension of Tanner graph that consists of check nodes and the information bit nodes used for detecting errors occurred in the distribution of key during the multicast communication. Pseudo encoding stopping set is similar to pseudo tree where two key check nodes are additionally introduced. Therefore, the key encoding module is mainly used to encode the keying information. This encoded information is directly sent to key generation and distribution module.
3.4 GROUP CENTER DATABASE

The group center database module is a storage area that stores the user name (Uname), password (Pwd), PK of each user, GK of each group, media information and group information. This module delivers the keys to key generation and distribution module and rekeying module whenever a change occurs in the group membership.

3.5 MEDIA SERVER

The media server has two important components namely media data manager and multicasting module. The media data manager is responsible for adding new multimedia data and deleting an existing data from the media server database which can be provided to the users. The data about members of different groups, SGK and GK are obtained from the GC and are stored in media server database by the media server. Moreover, it performs data scrambling operation used for scrambling the video data by using the GK which will be retrieved from media server database. The scrambled video data is sent to the multicast group members. All the communications which are taking place between different multicast groups are managed by this Multicasting module.

3.6 MEDIA SERVER DATABASE

The media server database is responsible for storing the multimedia information available in the media server. This repository is completely maintained by the media server. Therefore, the media server can add new services, delete services and update services. This database has information such as SGK, GK and media information.
3.7 THESIS CONTRIBUTIONS ON PROPOSED ARCHITECTURE

The major contributions of this research work are spread in the key generation and distribution module, group management module, rekeying module and key encoding module of the GC. In addition, in the user interface side, key recovery manager that uses two modules namely key updating and key decoding are newly proposed in this research work.

There are many contributions in this work with respect to the system architecture. First, the integration of user registration, login, user administration, key recovery and data descrambling in to the user interface enables the user activities to be effective and secure. This is because the registration module helps to perform authentication. Moreover, the key recovery manager is directly connected with registration module. From the experiments conducted in this work, it has been observed that

- Authentication must be performed by the user interface.
- Two separate databases are necessary one for storing media and group related information in the GC database and other for storing user related information in the user database.
- The GC must have separate modules for key generation, key distribution and group management.

Second, the group center is given verification, key distribution, group management and key encoding. Third, media server is provided for server side. Finally, databases are provided to store keys and media information. Hence, the major contributions of this research work are spread in the key generation and distribution module, group management module, rekeying module and key encoding module of the GC. In addition, in the user
interface side, key recovery manager that uses two modules namely key updating and key decoding are also newly proposed in this research work. The major assumptions made in the design of this system are:

- The system can support several thousands of users.
- The GC keeps all private keys secret and each user keeps their own private keys secret.
- User joining and leaving behavior is independent of other users.
- GC is trusted such that they never fail and nobody can compromise it.