Access control and authentication rely on and co-exist with other security services in computer system. The responsibility of an authentication service is to correctly establish the identity of the legitimate user. The access control is concerned with the legal users' access privileges. After successful verification of a legal user identity by the authentication service, the access control will be enforced. There are several potential security risks in protecting data and providing access control over the data. In addition, due to the rapid development of wireless networks and cloud environments, the users have access to remote servers through open channels. Thus, authentication plays a major role in distributed computer networks to ensure the legitimacy of users for protecting resources from unauthorized access by means of providing a variety of security services to the users, such as user credentials' privacy, session key security, and mutual authentication. Moreover, several circumstances require that the revocation mechanism needs to revoke the illegal/compromised users and servers before their intended expiration dates. As a conclusion, it is a challenging problem to manage dynamically the access rights to the resources and protect them from unauthorized access.

In first study, we propose a novel dynamic hierarchical key management mechanism for the mobile agents in a distributed network environment using symmetric-key cryptosystem and elliptic curve cryptography (ECC) based signature (El-Gamal type). In second study, we propose a new key management scheme for dynamic access control in a large leaf class hierarchy, which makes use of symmetric-key cryptosystem and one-way hash function. In third study, we propose a novel time-bound hierarchical access control scheme for secure broadcasting, in which each user needs to store a distinct and unique private key, and hence each user in a channel group can subscribe for an individual channel. In fourth study, we propose a new secure elliptic curve cryptography (ECC) based SSO (single sign-on) mechanism for user authentication and key establishment for the secure communications in a distributed computer networks using biometric-based smart card. Finally, we concentrate on designing a new secure multi-server authentication protocol using biometric-based smart card and ECC with more security functionalities.