the devices connected to it. As it serves as an aggregation point for an edge, the gateway has a very important security role in the ecosystem.

An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. Also, the authentication mechanism for the edge components should be as strong as any other component in the framework. Where ever possible the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

- **Cloud Platform**

  In an IoT ecosystem, the cloud component is referred to as the main central aggregation and data management point. Access to the cloud is restricted. The cloud component is usually at higher risk as it the central point of data aggregation for most of the data in the ecosystem. It also includes command and control (C2) component which is a centralized computer that issues various commands for the distribution of extensions and updates.

  A secure framework for the cloud component should include encrypted communications, strong authentication credentials, secure web interface, encrypted storage, automatic updates and so on.

- **Mobile**

  In an IoT ecosystem, the mobile interface plays an important part particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. Some mobile applications provide the users only limited data from specific edge devices while others allow the complete manipulation of the edge components. Proper attention should be given to the mobile interface as they are prone to various cyber-attacks.

  An ideal framework for the mobile interface should include proper authentication mechanism for the user, account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels and the security of the data transmitted over the channel.