**SYSTEM ANALYSIS:**

**EXISTING SYSTEM**:

A QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are unsuitable for storing secret data. During the past few years, many efforts have been made to place and protect secret messages in QR codes. Some scholars have utilized traditional steganography or watermarking techniques [6]–[8]. These studies embed a QR code as a secret into a mask image; or treat it as a mask to hide information. Secret extraction in both techniques requires a transformation to one specified domain, such as DCT or DWT. Regarding secret sharing methods, a polynomial

algorithm was presented in [9], where shadows were conveyed in the form of QR codes. In this scheme, the QR code was used as an information carrier to transfer shadow information and its message is meaningless. The authors of presented a scheme that can resist print-and-scan operations and detect cheaters. Additionally, a novel QR code was designed for two-level message sharing and document authentication in which a hash function is performed when decrypting the secret. Compared with Boolean operations, the computational overhead of all the aforementioned schemes is slightly larger

**PROPOSED** **SYSTEM**:

In this project, an innovative scheme is proposed to improve the security of QR codes. First, an improved (*n*, *n)* sharing method is designed to avoid the security weakness of [26]. On this basis, we consider the method for (*k*, *n)* access structures by utilizing the (*k*, *k)* sharing instance on every *k*-participant subset, respectively.

This approach will require a large number of instances as *n* increases. Therefore, we further present two division algorithms to classify all the *k*-participant subsets into several collections, in which instances of multiple subsets can be replaced by only one.

One significant feature of QR codes is the error correction capability, which allows QR code readers to correctly decode data, even when parts of the symbol are dirty or damaged. The Secret Message is Encoded or Encrypted into another form by using AES Algorithm. Then the Encrypted message is splits into four shares and stored in different QR Code image. Then it will send to the user. In user part, we have to merge all the QR code and by using the QR code scanner, original message is retrieved.

**Advantages**:

* More Secure and safe
* Third party and malicious user cannot detect the original data.