3.3 Security notes

The following security measures will enter the design/development phase to be realized:

• Authentication: User accounts must be secured by a secure login with robust password policies that include a two-factor authentication.

• Authorization: Role-based access control must provide access to sensitive information to users authorized and restrict actions authorized users can do on application data.

• Data Encryption: All sensitive data (like credentials and sensitive user information) must be encrypted in transit by its travel mediums (HTTPS) (encrypting data in transit) and at rest in the database storage (encrypting data at rest).

• Input Validation: Input validation mechanisms must be effectively in place to protect against common attacks, like, SQL injections, cross-site scripting (XSS), and injection-based attacks.

• Session Management: It must possess secure session management with session timeouts and token-based authentication controls so as to thwart session hijacking, and MITM attacks (man in the middle).

• Privacy Compliance: The system must comply with applicable data protection and privacy laws/regulations (e.g., GDPR) so that data will be processed accordingly.