3.2.1 External Requirements

3.2.1.1 Security

Security is an important aspect of game development, and it is essential to ensure that the game is secure and does not pose any risks to the players. The following measures will be taken to ensure the security of the game:

- **Data encryption:** All sensitive data such as user credentials, payment information, and other personal information will be encrypted to prevent unauthorized access.
- **Access controls:** Access to the game servers and databases will be restricted only to authorized personnel to prevent data breaches and unauthorized access.
- **Anti-cheat mechanisms:** The game will include anti-cheat mechanisms to prevent cheating, hacking, and other malicious activities that may compromise the security of the game.

3.2.1.2 Protection

- **Code obfuscation:** The game's code will be obfuscated to make it harder for hackers to reverse engineer and steal intellectual property or manipulate game data.
- **Encryption:** Game data, including user data and game files, will be encrypted to prevent unauthorized access.
- **Anti-cheat measures:** The game will implement anti-cheat measures to detect and prevent cheating and unfair gameplay, such as using third-party software or exploiting bugs.
- **User account security:** User accounts will be secured with strong passwords, two-factor authentication, and other security measures to prevent unauthorized access and protect user data.

3.2.1.3 Authorization and Authentication

Authentication is the process of verifying a user's identity. In games that involve user accounts, developers need to implement secure authentication mechanisms to prevent unauthorized access to user accounts and protect sensitive user data. This includes things like implementing strong password requirements, two-factor authentication, and session management to prevent session hijacking.

Authorization is the process of granting or denying access to specific resources or functionality based on a user's identity and permissions. In games that involve online multiplayer functionality or social features, developers need to implement authorization mechanisms to control what actions users can perform in the game, what data they can access, and who they can interact with. This includes things like implementing role-based access controls, establishing user permissions, and implementing appropriate validation and error handling mechanisms to prevent unauthorized actions.

Social authentication allows users to log in to the game using their social media accounts,

such as Facebook or Google. Developers need to ensure that their social authentication mechanisms are secure and comply with relevant regulations and standards, such as OAuth and OpenID Connect. This includes things like implementing secure data exchange between the game and the social media platform, handling user consent and permissions, and implementing appropriate error handling and logging mechanisms.