# Threat Model

## 4.1 Threat actors

Possibilities where a threat can be posed from possible persons or organisations to the application are as follows:

* Modifications to the system
* Access to private or sensitive information like an account number for example.
* Exploit, change and delete bank account details or change them
* Securing the data to protect against SQL Injection via attacks.

## 4.2 Assumptions

* Banking software will have up to date software for authentication via security to identify users’ identity.
* All sensitive data will be encrypted for security of information and the files will deleted when finished.

## 4.3 Thrust Boundaries

* **Application Users:** The users that use the application.
* **Application Device:** the device running the console app.

## 4.4 Threat Assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Category | Trust Boundary | Threat Description | Action | Action Description |
| 1 | Spoofing | Application Device | Access to account information like AccNo and potential fraud. | Migrate | All data will be encrypted and not saved and so encrypted data would be useless to attackers. |
| 2 | Spoofing | Application Device | Virus or Malware on user’s device with file being used by application | Transfer | Antivirus software installed on device to protect against it. |
| 3 | Tampering | Applications Users | Attackers gain access to a user’s account | Accept | The attacker must also access to the machine running the application as all data is stored locally. Even should this occur, only an admin has the ability to modify any data. |
| 4 | Repudiation | Application Device | Admin creates, modifies a account and denies doing so | Accept | The attacker must have access to machine running the application. The logs can be decrypted at any given time by admin in order to investigate claims. |

## 4.5 Threat Model Diagram

Diagram

Description automatically generated