Given the security case pattern for an Instant messaging (IM) software, I will instantiate the pattern based on the domain information provided:

Hierarchy Visualization of the Security Case:

```

- G1: Instant messaging software is acceptably secure in the instant messaging system

- C1: Definition and description of Instant messaging software

- C2: Definition and description of the instant messaging system

- C3: 'Acceptably secure' is defined as ensuring protection against unauthorized access and data breaches

- S1: Argument that software assets are under protection

- J1: Protection of software assets supports that software is acceptably secure

- G2: All identified software critical assets are protected

- C4: List of Instant messaging software critical assets (Registration info, Registration process, User account information, Authentication information, Login process, Chat logs)

- J2: Relationship between assets is clear and can be argued separately

- S2: Respective arguments of software critical assets

- G3: Registration information is protected

- S3: Argument of the type which the software critical asset belongs to

- C5: List of software critical asset types in PEDD (Process, Environment Entity, Data Exchange, Data Storage)

- J3: Types of software assets are according to PEDD

── G4: Registration information which belongs to Data Storage is protected

- G3: Registration process is protected

── G4: Registration process which belongs to Process is protected

- G3: User account information is protected

── G4: User account information which belongs to Data Storage is protected

- G3: Authentication information is protected

── G4: Authentication information which belongs to Data Exchange is protected

- G3: Login process is protected

── G4: Login process which belongs to Process is protected

- G3: Chat logs are protected

── G4: Chat logs which belong to Data Storage is protected

```

This hierarchy specifies a security case for an IM software ensuring that all critical assets are detailed with their protection mechanisms and they are aligned according to the types specified by PEDD. Each goal, strategy, and context supports the overall security claim, backed by justifications ensuring a comprehensive approach to safeguarding the application.