Based on the provided security case pattern, here is the instantiation of a security case for Instant Messaging (IM) software, laid out in a hierarchy resembling a tree format. Each critical asset and its associated elements are expanded according to the pattern and the specific information on IM software given in the domain information.

@Assurance\_case

- G1: IM software is acceptably secure in the operational environment.

- C1: IM software includes all features such as message sending, file sharing, etc.

- C2: Operational environment includes all platforms on which the IM software runs.

- C3: Acceptably secure means protection against unauthorized access, data breaches, and ensuring data integrity and confidentiality.

- S1: Argument that IM software assets are under protection.

- J1: Protecting all assets of the IM software ensures the overall security of the software.

- G2: All identified IM software critical assets are protected.

- C4: List of critical assets includes Registration information, User account information, Authentication information, Login process and Chat logs.

- J2: Each asset can be protected with specific security controls making the relationship clear.

- S2: Respective arguments of IM software critical assets.

- G3: User account information is protected.

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

- C5: Types include Data Storage and Data Exchange.

- J3: Proper classification of assets according to PEDD ensures targeted protection measures.

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

- G3: Authentication information is protected.

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

- G4: Authentication information which belongs to Data Storage is protected.

- G3: Login process is protected.

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

- G4: Login process which belongs to Process is protected.

- G3: Chat logs are protected.

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

- G4: Chat logs which belong to Data Storage is protected.

@End\_Assurance\_case

- This security case provides a structured and detailed account ensuring the security of critical assets in Instant Messaging software by categorizing them according to the PEDD classification (Process, Environment Entity, Data Exchange, Data Storage) and arguing for their protection at each level of the hierarchy. Each goal and strategy is supported with context and justification to reinforce the robustness of the security strategy applied.