Supplementary Requirements Documentation – Server & Database Subsystems

Smart House

Revision History

Date	Version	Description	Author
06/02/26	1.0	Initial supplementary requirements focusing on database POV	Katerina Arvay, Dario Ostojic, Andre Sandblom

Supplementary Requirements List

Supplementary Requirement Name	Priority
S1. Data persistence & consistency	Essential
S2. Database performance & latency	Essential
S3. Scalability of data storage	Essential
S4. Data security & access control	Essential
S5. Backup & recovery strategy	Essential
S6. Availability & fault tolerance	Desirable
S7. Database technology constraints	Optional

Supplementary Requirements Descriptions

S1. Data persistency & consistency

All smart home data, including user accounts, smart devices, device states, schedules, and historical logs, shall be persistently stored in the database. The database must ensure data consistency, meaning that stored device states accurately reflect the real-world state of devices after successful operations. Transactions should be handled in a way that prevents partial or inconsistent updates.

S2. Database performance & latency

Database operations related to critical functionality, such as retrieving device status or updating device states, shall respond within a maximum of 2 seconds under normal operating conditions. The database should efficiently support frequent read and write operations generated by multiple users and smart devices simultaneously.

S3. Scalability of data storage

The database shall support scalability to handle an increasing number of users, smart devices, automation rules, and sensor data over time. The system should allow expansion without requiring major architectural changes or service interruptions.

S4. Data security & access control

The database shall enforce strict access control to ensure that users can only access data related to their own smart home environment. Sensitive information such as user credentials must be securely stored using appropriate protection mechanisms (e.g., password hashing). Database access shall be limited to authorized system components only.

S5. Backup & recovery strategy

The system shall implement automated and regular database backups to prevent data loss. In the event of system failure, corruption or accidental data deletion, the database must be recoverable to a recent consistent state with minimal loss of data.

S6. Availability & fault tolerance

The database should be designed to minimize downtime and support continuous operation. Where possible, fault-tolerance mechanisms such as replication or redundancy may be used to ensure system availability in case of hardware or software failures.

S7. Database technology constraints

The system may use either a relational or non-relational database solution depending on performance, scalability, and data structure requirements. The chosen database technology should support structured storage of users, devices, configurations and logs, and integrate smoothly with the rest of the smart home system.