ATM system

database requirements

the requirements will be numbered to represent their requirement ID.

**Functional Requirements**

1. The database must be able to store and verify user identity using card and PIN.
2. The database must be able to store and retrieve account balance information.
3. The database must be able to store details of cash withdrawals.
4. The database must be able to store details of cash deposits.
5. The database must be able to store details of fund transfers.
6. The database must be able to store and manage user session information securely.
7. The database must be able to record and store error logs for auditing and troubleshooting.
8. The database must be able to store and enforce daily withdrawal and transaction limits.
9. The database must be able to store and retrieve a summary of recent transactions (mini statement).
10. The database must be able to store records of PIN changes.
11. The database must be able to generate and store detailed account statements.
12. The database must be able to handle and store card-related operations like blocking lost/stolen cards.
13. The database must be able to manage and store different currencies for international transactions.
14. The database must be able to store and retrieve transaction receipt information.
15. The database must be able to store and manage ATM machine status data.
16. The database should be able to store and retrieve user preferences for language selection.
17. The database should be able to store and manage fee calculation data.
18. The database should be able to store and manage compliance data for regulatory reporting.
19. The database should be able to store and manage data for fund transfer limits.
20. The database should be able to store and manage data for multi-factor authentication.
21. The database should be able to store a user’s address.
22. The database should be able to store a user’s date of birth.

**Non-Functional Requirements**

1. The database must ensure data encryption, secure authentication, and protection against fraud.
2. The database must provide quick response times for all database queries and transactions.
3. The database must ensure high availability and minimal downtime.
4. The database must support increasing numbers of users and transactions.
5. The database must allow easy updates and maintenance of the database system.
6. The database must ensure data integrity and consistency.
7. The database must be compliant with relevant industry standards and regulations.