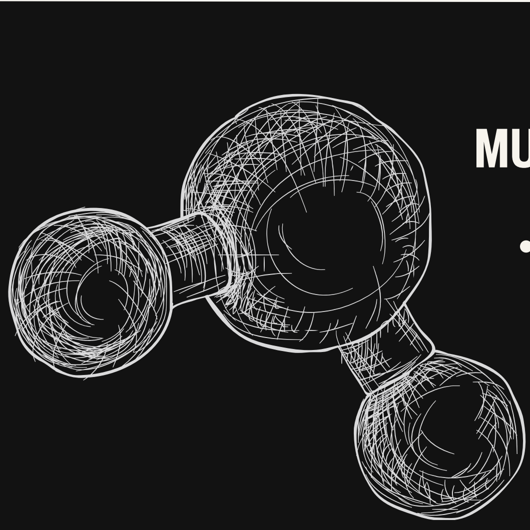
Infographic Outline:

A Model of Atomicity for Multilevel Transactions



1

MULTILEVEL TRANSACTION ATOMICITY

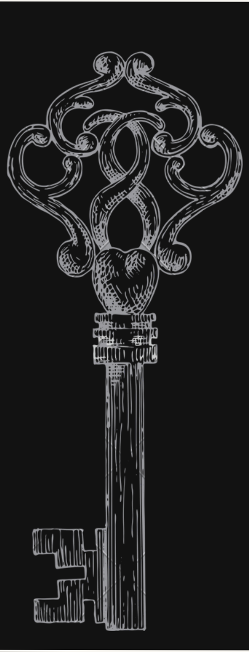
- **Ensuring Data Integrity in Secure Multi-Layered Systems.**

Traditional atomicity fails in Multilevel Secure (MLS) databases because high-level transactions cannot "lock" low-level data without creating security leaks (Covert Channels).

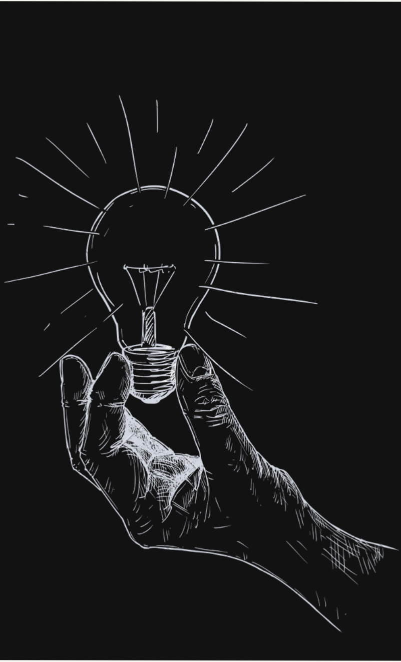
CORE CONCEPTS

- **Key Definitions.**

- Multilevel Security (MLS): Data is classified into different sensitivity levels (e.g., Unclassified, Secret, Top Secret).
- Atomicity: The "All or Nothing" property. Either all parts of a transaction happen, or none do.
- The Conflict: High-level processes need to read/write low-level data, but low-level processes must remain unaware of high-level activities.



2



3

THE MODEL'S SOLUTION

- **Transaction Decomposition.**

Part A: Transaction Decomposition

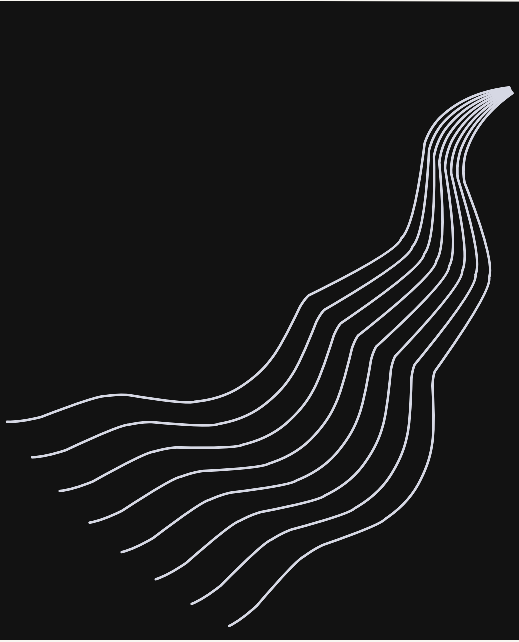
- Transactions are broken down into single-level subjects.
- A "Multilevel Transaction" is seen as a set of related sub-transactions operating at different security levels.

- Part B: The Execution Strategy
- Bottom-Up Execution: Operations at lower security levels must be verified before higher-level operations proceed.
- Correctness Criteria: The model ensures that even if a high-level part fails, the low-level data remains consistent.

EXECUTION FLOW

- **The "Bottom-Up" Strategy.**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla accumsan nisl sit amet faucibus accumsan. Aliquam fringilla erat non est blandit.



4

5

FINAL IMPACT

- **Integrity Without Compromise**

- **Atomicity**: The system remains consistent even if a failure occurs.
- **Confidentiality**: No "Read Up" or "Write Down" rules are violated.
- **Conclusion**: High-assurance security and database reliability can coexist.