RNS Trust ®

RNS Institute of Technology

Autonomous Institute of Technology Affiliated to VTU
Accredited with NAAC A+ Grade

PRIVACY-PRESERVING HEALTH DATA EXCHANGE USING SECURE MULTI-PARTY COMPUTATION(MPC)

TEAM :14

K LOKESH CHOWDARY 1RN22CY023

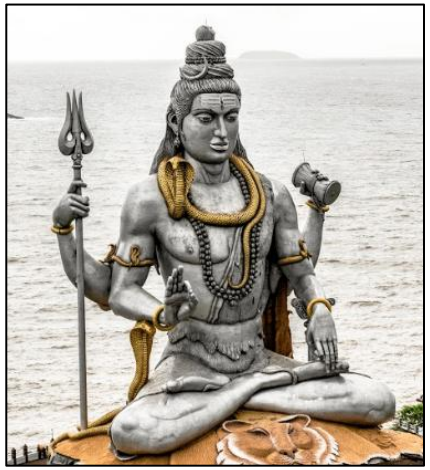
SHASHANK L 1RN22CY035

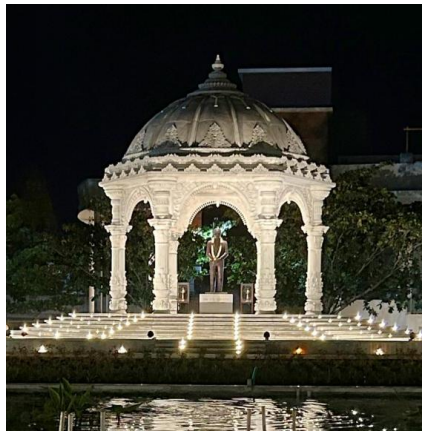
Guide : Mrs Latha P

Project Coordinator

Dr R Rajkumar

Associate Professor





23
Years of
Academic Excellence
RNS INSTITUTE
OF TECHNOLOGY

Tribute to Our Founder

Dr. R N Shetty
Founder
1928 - forever

Agenda

- Problem Statement
- Proposed Solution
- Project Status
- Technical Architecture
- Multi-Layered Security Approach
- Core Features
- SMPC Workflow
- Live Demonstration
- Impact & Significance
- Conclusion

Problem Statement

Data Silos in Healthcare

- Healthcare data is fragmented across different institutions, creating **data silos**.
- Strict privacy regulations like **HIPAA and GDPR** limit data sharing, which is crucial for research.
- This lack of access to diverse datasets **slows down medical research**, hinders innovation, and can negatively impact patient outcomes.
- **The core challenge:** How can we enable collaborative research while guaranteeing patient privacy?

The Solution: Collaborative Analysis, Guaranteed Privacy

- We've developed a platform that allows institutions to **collaborate on sensitive data without ever exposing it**.
- **The core technology:** Secure Multi-Party Computation (SMPC).
- **How it works:** Multiple parties can jointly compute a function over their private inputs (e.g., calculate the average age of patients in a study) without revealing those inputs to each other.

- **Key Benefits:**
  - No raw data is ever shared.
  - Fully compliant with HIPAA/GDPR.
  - Enables powerful, multi-institutional research.

Project Status: Ready for Demonstration

➢**Overall Completion: 85%**

- **Completed Milestones:**
  - Core Platform Infrastructure
  - Multi-Layered Security Implementation
  - Data Management & API Endpoints

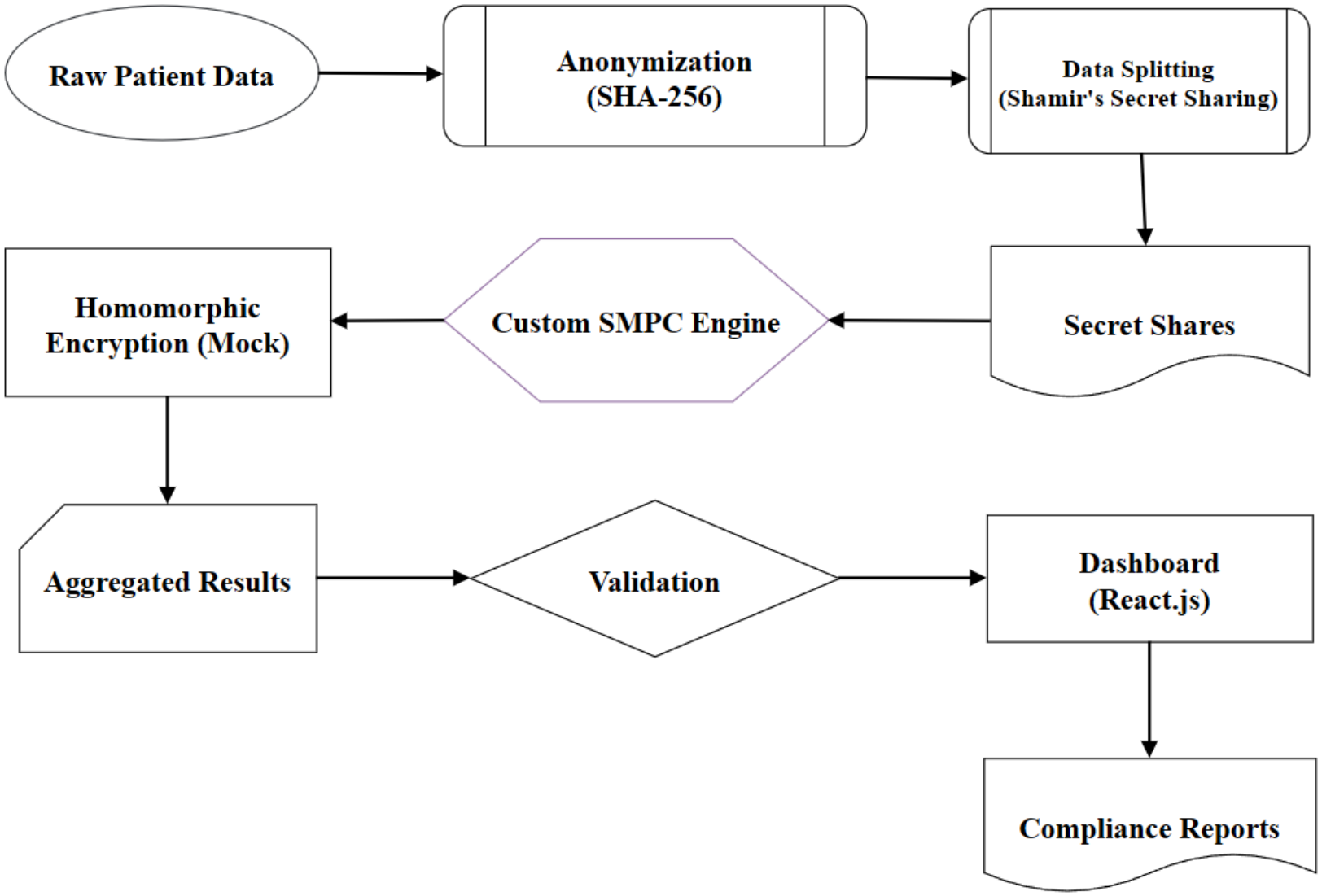
- **In Progress:**
  - Advanced Analytics Features
  - Real-time Collaboration UI

➢**Status:** We have a **working prototype ready for a live demonstration**.

Technical Architecture

1.	Frontend	Next.js, React, TypeScript
2.	Backend	FastAPI (Python)
3.	Privacy-Preserving Crypto	Shamir's Secret Sharing (SSS)
4.	Core Security	Secure Multi-Party Computation, Homomorphic Encryption, JWT Authentication
5.	Database	SQLite (PostgreSQL for production)
6.	Real-time	WebSockets

BLOCK DIAGRAM



A Multi-Layered Security Approach

Our platform is built with a **defense-in-depth** strategy, securing data at every level.

- **Layer 1: Application Security**
  - Role-Based Access Control (**RBAC**) and **JWT** Authentication.
- **Layer 2: Data Security (The Core)**
  - **Secure Multi-Party Computation (SMPC)** and **Homomorphic Encryption (HE)** to protect data during computation.
- **Layer 3: Transport Security**
  - TLS/SSL encryption for all data in transit.
- **Layer 4: Infrastructure Security**
  - Database encryption at rest and comprehensive audit logging

Core Features

➢**Secure Computation Engine:**

- Allows users to perform statistical analysis (mean, median, variance) on combined datasets without sharing raw data.
- Supports multiple security levels for flexibility.

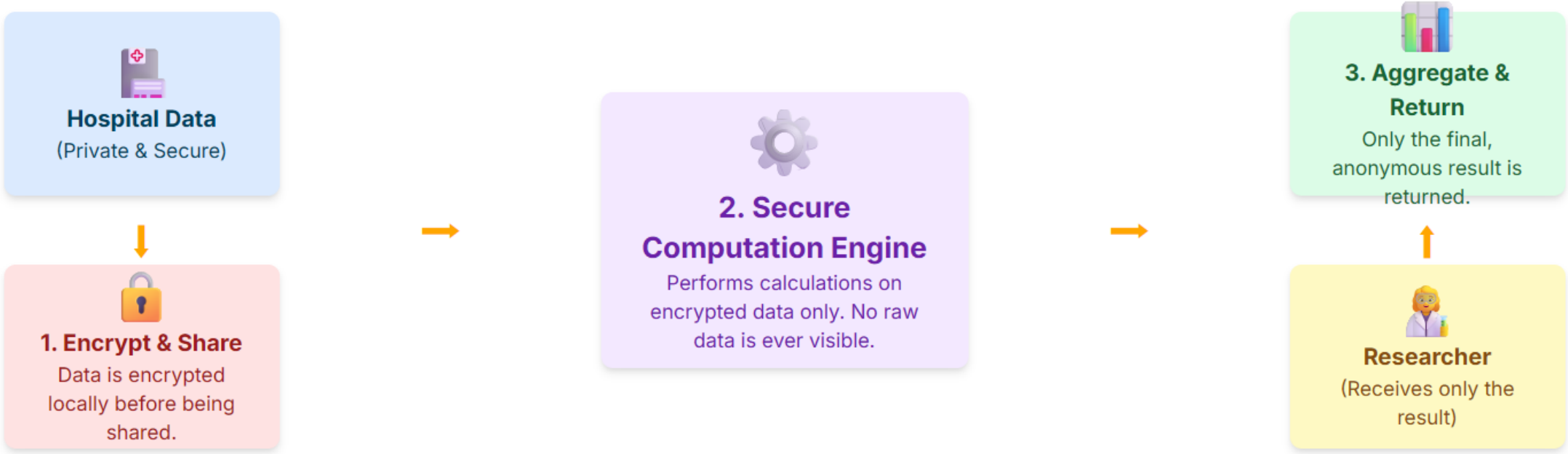
➢**Role-Based Access Control (RBAC):**

- Defines specific permissions for different user types (e.g., Hospital, Researcher, Lab) to ensure users only see what they're authorized to.

➢**Real-Time Analytics Dashboard:**

- Visualizes aggregated results as they are computed.
- Allows secure export of results (not raw data) in JSON/CSV.

How SMPC Works: A Simplified Workflow



Impact & Significance

➢**For Healthcare & Research:**

- Unlocks the potential of siloed health data for large-scale studies.
- Accelerates medical discoveries while strengthening patient privacy.

➢**For Technology:**

- Provides a practical, real-world application of advanced cryptographic techniques like SMPC.
- Creates a scalable and compliant architecture for secure data collaboration in any regulated industry.

Conclusion & Future Work

➢**Conclusion:** We have successfully built a functional platform that solves the critical challenge of sharing health data for research while ensuring patient privacy.

➢**Next Steps:**

- **Performance Optimization:** Further enhance computation speed.
- **Advanced Analytics:** Integrate Machine Learning model training on encrypted data.
- **Production Deployment:** Move to a scalable cloud infrastructure.

ESTD : 2001
An Institute with a Difference

THANK YOU