Milestone 2 Progress Evaluation

Project Ragnarok: Post-Quantum Cybersecurity with Lightning Data

Group Members

- Joanna Zhang (zhangj2022@my.fit.edu)
- Gianni Bubb (gbubb2022@my.fit.edu)
- Aidan Nelappana (anelappana2021@my.fit.edu)

Advisor / Client

- Dr. Bhattacharyya, sbhattacharyya@fit.edu
- Dr. Amitabh Nag

Institution: Florida Institute of Technology – Senior Design

1. **Progress of Current Milestone (Progress Matrix)**

Task	Completion %	Aidan	Gianni	Joanna	To Do
1. Implement basic Python API	100%	100%	0%	0%	Completed core API structure and request handling
2.Backend integration	80%	40%	20%	20%	Resolve async issues and ensure full module communication
3.Post-Quantum algorithm implementation	70%	30%	40%	0%	Optimize performance and complete remaining algorithms
4.Database security fixes	90%	0%	10%	80%	Conduct final testing and validation

2. **Discussion of Accomplished Tasks**

Task 1:Thor Migration Development

We ported the original Thor platform into Rust by rebuilding the server-side functionality as an Axum web application backed by PostgreSQL, while preserving the existing website as static frontend assets served by the new backend. The legacy lightning-data workflow was carried over through CSV import tooling, and the original key-generation and file-encryption ideas were reimplemented as Rust API routes and services. On top of the port, we modernized the stack by adding structured database migrations, Docker support, input validation, bearer-token protected routes, entropy analysis, and teammate-friendly setup scripts so the platform is easier to run, extend, and develop across environments.

Task 2: Backend Integration

Significant progress was made in integrating the backend components, including connecting the API with the database and cryptographic modules. This process involved ensuring that data flows correctly between services and that asynchronous operations are handled efficiently. We encountered challenges related to synchronization and error propagation, particularly when dealing with database queries and external modules. These issues were addressed through debugging, restructuring function calls, and improving error handling to ensure reliable system behavior.

Task 3: Post-Quantum Algorithm and Entropy testing Implementation

We implemented initial versions of post-quantum cryptographic algorithms based on NIST-aligned standards. This required researching appropriate algorithms, understanding their structure, and adapting them into the system. The complexity of these algorithms presented challenges, particularly in ensuring correctness and compatibility with existing modules. Despite these challenges, we successfully integrated basic functionality and established a foundation for further optimization and testing in future milestones.

Task 4: Security Improvements

A major focus of this milestone was improving system security, particularly at the database level. We implemented role-based authorization to restrict access to sensitive operations, ensuring that only permitted users can perform actions such as key generation and file encryption. In addition, input validation was introduced to verify that all user-provided data meets expected formats and constraints, preventing invalid or malicious input. Error handling was also enhanced using a structured approach, improving both security and system reliability. These improvements significantly strengthen the overall security posture of the system.

3. Team Member Contributions

Aidan Nelappana: Worked on porting the original Thor platform into a Rust/Axum webserver backed by PostgreSQL, while preserving the website as a static frontend served through the new backend. I implemented and integrated core backend functionality including API routes, database connectivity, legacy lightning-data import support, authentication improvements, input

validation, file encryption workflows, and entropy analysis features. I also started work on NIST SP 800-90B-inspired entropy analysis and early Open Quantum Safe wrapper integration, helping lay the groundwork for stronger randomness evaluation and future cryptographic expansion. In addition, I improved the team's development workflow through Docker support, setup scripts, smoke-test tooling, and clearer documentation so the rest of the team could run, test, and build on the system more easily.

Gianni Bubb: Led the development of API endpoints and routing, making sure the system components interacted efficiently. I also worked on implementing post-quantum algorithms and integrating different modules into a cohesive system. My role involved both designing the architecture and ensuring that the system's performance and security requirements were met.

Joanna Zhang: Focused on improving the system's security. I worked on database security enhancements, input validation, and authorization protocols, ensuring that our platform was protected against potential vulnerabilities. Additionally, I documented the rationale behind each security measure and updated the system design to reflect these improvements, helping maintain clarity and structure for the team.

Plan for Next Milestone (Task Matrix)

Task	Aidan	Gianni	Joanna
1.Complete backend integration	Finalize API-to-database connections and fix remaining bugs	Assist with debugging and ensure routing stability	Verify secure data handling and validate inputs
2.Optimize PQ algorithms	Assist with testing and benchmarking	Improve algorithm efficiency and correctness	Document performance results and security implications
3.Finalize API & routing	Support endpoint testing and integration	Complete all routes and ensure proper request handling	Perform security testing on endpoints
4.Strengthen security controls	Assist with testing security features	Support implementation of secure practices	Implement additional validation, authorization checks, and system hardening

Discussion of Planned Tasks

Task 1: Backend Completion

In the next milestone, we plan to complete backend integration by ensuring that all components work together seamlessly. This includes finalizing connections between the API, database, and cryptographic modules, as well as resolving any remaining bugs. Additional effort will be placed on improving system performance and ensuring that asynchronous operations are handled efficiently. The goal is to achieve a stable and fully functional backend that supports all required features.

Task 2: Algorithm Optimization

We will focus on optimizing the implemented post-quantum algorithms to improve performance and efficiency. This involves refining the implementation, reducing computational overhead, and conducting thorough testing to ensure correctness. Benchmarking will also be performed to evaluate performance under different conditions. These improvements are essential to ensure that the system can handle real-world workloads effectively.

Task 3: API Finalization

All API endpoints will be finalized and thoroughly tested to ensure they function correctly and handle various edge cases. This includes verifying request and response formats, improving routing logic, and ensuring consistent behavior across all endpoints. Additional testing will be conducted to simulate real-world usage scenarios, ensuring that the API is robust, reliable, and ready for demonstration.

Task 4: Security Enhancements

We will continue to strengthen system security by implementing additional controls and hardening measures. This includes expanding input validation, refining authorization checks, and addressing any remaining vulnerabilities. Security testing will also be conducted to identify potential weaknesses and ensure that the system is resilient against common attacks. These efforts will further improve the reliability and trustworthiness of the system.

Meetings

Client Meeting Date(s)

March 11, 2026

Client Feedback

See Faculty Advisor Feedback below.

Faculty Advisor Meeting Date(s)

March 11, 2026

Faculty Advisor Feedback

- **Task 1:**
- **Task 2:**
- **Task 3:**
- **Task 4:**

Faculty Advisor Signature: _____ Date: _____

Evaluation by Faculty Advisor

- Faculty Advisor: detach and return this page to Dr. Chan (HC 209) or email the scores to pkc@cs.fit.edu
- Score (0-10) for each member: circle a score (or circle two adjacent scores for .25 or write down a real number between 0 and 10)

Joanna Zhang	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
Gianni Bubb	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
Aidan Nelappana	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10

Faculty Advisor Signature: _____ Date: _____