Milestone 1 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: Dr. Bhattacharyya, sbhattacharyya@fit.edu

Client: Dr. Bhattacharyya, sbhattacharyya@fit.edu

Institution: Florida Institute of Technology – Senior Design

1. Progress of Current Milestone

Task No.	Task Description	Completion %	Joanna	Gianni	Aidan	To Do / Issues
1	Investigate tools	90%	10%	40%	40%	Look into Project Thor
2	Hello World demos	30%	0%	15%	15%	Adjust as the project is refined
3	Requirements Document	100%	33%	33%	33%	Adjust as the project is refined

4	Design Document	100%	33%	33%	33%	Adjust as the project is refined
5	Test Plan	100%	50%	50%	0%	Adjust as the project is refined
6	Implement, test & demo feature/module	30%	10%	10%	10%	Adjust as the project is refined

2. Discussion of Accomplished Tasks (Current Milestone)

Task 1: Investigate Tools

We attempted to run Project Thor but could not get the website to generate a key. We were advised to convert project Thor's frontend from PHP to HTML. In terms of new tools, we decided to evaluate potential API frameworks by what security features are offered, quality of documentation, database connection features, and performance. We did not get to do enough testing but we looked at FastAPI, web2py, flask, and py4web. Currently we are deciding to use FastAPI.

Task 2: Hello World Demos

We developed a simple "Hello World" prototype to validate that the backend environment was properly configured and operational. Using FastAPI, we set up a demo development server and successfully implemented a basic GET request. This confirmed that the server could start correctly, handle requests, and return responses, establishing a working foundation for further development.

Task 3: Requirements Document

The system scope and key use cases were defined and organized in the Requirements Document to establish a clear project foundation. The requirements were reviewed for alignment with

project goals and may be refined as we gain deeper insight into API and database security. The document will continue to evolve as the project vision becomes more defined.

Task 4: Design Document

We organized the design of the product into a layered architecture. We developed prototype design models, and described our post-quantum cryptographic algorithm design. This document will continue to be refined along with the project.

Task 5: Test Plan

The test plan pulls from the requirements and covers various important test cases. This document will continue to be evaluated and added to as the project progresses. It will also reflect any changes made to the requirements.

3. Team Member Contributions (Current Milestone)

Joanna Zhang: For the current milestone, I worked on all major project documentation, including the Requirements Document, Design Document, and Test Document. I initiated the development of the Requirements, Design, and Test documents by setting up their structure and inputting the appropriate project information according to the system specifications and guidelines. I ensured the documents were properly formatted, organized, and aligned with one another for consistency and traceability. I also organized and scheduled group meetings using Google Calendar to maintain clear communication and keep the team on track with deadlines. Additionally, I concentrated on researching the system's security architecture and analyzing the previous Project Thor implementation to better understand its security framework and apply relevant insights to strengthen our current project design.

Gianni Bubb: I researched API frameworks and API security. I gathered potential API frameworks. I organized and formatted our collaboration infrastructure. In the google drive I created the outline of documents and the presentation required for Milestone 1. I helped format the requirements document, added some important requirements and added new sections. I made sure certain sections were filled with the correct information and the document reached expectations. For the design document, I created the architecture diagram and wrote the web interface section. I also looked into Project Thor's implementation and setup.

Aidan Nelappana: For Milestone 1, I focused on developing the formal theoretical and cryptographic foundation of Project Ragnarok. I contributed to the design of the system's security model by defining adversarial assumptions and outlining how lightning-derived entropy can be transformed into cryptographically secure randomness under both classical and quantum threat models. I conducted research into post-quantum cryptographic (PQC) algorithms,

including lattice-based key encapsulation mechanisms and signature schemes recognized in the NIST Post-Quantum Cryptography standardization process (e.g., ML-KEM and ML-DSA). Based on this research, I contributed to defining the system's cryptographic direction and ensuring that our architecture supports cryptographic agility for future algorithm updates. I worked on drafting and refining the Requirements and Design Documents, particularly sections involving entropy extraction, randomness conditioning, and formal security guarantees. I helped formalize the use of entropy extraction techniques consistent with the Leftover Hash Lemma and ensured that our design aligned with NIST standards for entropy estimation and post-quantum security. Additionally, I finalized all milestone documentation prior to submission, ensuring consistency between the Requirements, Design, and Test Documents, correcting technical language, and verifying that the documents aligned with formatting and project guidelines.

4. Plan for the Next Milestone

4.1 Task Matrix (Next Milestone)

Task No.	Task Description	Joanna	Gianni	Aidan
1	Implement, test & demo basic Post-Quantum (PQ) encryption integrated with entropy-enhanced key generation	Research integration, document implementation, assist testing	Implement PQ algorithms and backend integration	Implement entropy maximization logic and mathematical validation
2	Implement and test basic Python API with database security improvements	Refine requirements/design updates, document API & security controls	Implement API endpoints and connect to key generator	Strengthen database security, perform testing and remediation

4.2 Discussion of Planned Tasks (Next Milestone)

Task 1:
The goal is to implement and demonstrate basic post-quantum encryption integrated with our entropy-enhanced key generation. We will finalize entropy validation methods and connect them with selected PQ algorithms aligned with the National Institute of Standards and Technology guidelines. Risks include integration challenges and limited experience with PQ cryptography. Deliverables include a working demo and entropy test results.

Task 2:
The goal is to implement a basic Python API that securely provides access to generated keys while improving database security. We will develop API endpoints, connect them to the backend, and apply security fixes. Risks include configuration errors and integration issues. Deliverables include a functional API demo and validated database security improvements.

5. Client Interaction

Date(s) of Meeting(s) with Client During This Milestone:

- _____
- _____

Client Feedback on the Current Milestone:
See Faculty Advisor Feedback below.

6. Faculty Advisor Interaction

Date(s) of Meeting(s) with Faculty Advisor During This Milestone:

- _____
- _____

Faculty Advisor Feedback on Each Task

Task 1:
Feedback text.

Task 2:
Feedback text.

Task 3:
Feedback text.

Task 4:
Feedback text.

Faculty Advisor Signature: _____ Date: _____

1. 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: _____