1. **Team Members:**
   Sowmya Shetty
   Alem Abreha

2. **Title of Project:**
   Erasure coding and AONT algorithm selection for Secure Distributed Storage

3. **Introduction and Motivation:**
   Data storage systems require security mechanisms to ensure confidentiality and privacy. Storing data in a distributed scheme will secure data in such a way that, data will remain secured even after the compromise of a considerable number of the nodes involved in the distributed storage scheme. In addition to this, the distributed storage scheme provides fault tolerance and resiliency, since data can be safely recovered even after the loss of nodes or data corruption under a specific tolerance level.

   Security of the system not only depends on encryption algorithm but also on AONT(All-Or-Nothing Transformation), hence makes the system more secure and reliable. Stored sensitive data can be recovered as long as number of available nodes is greater or equal to the threshold number.

   The Distributed Storage Scheme is practical because it can be applied for securely storing data in: Storage Area Networks, Network Attached Storages, Backup Systems, communication of secure and confidential information and many other applications.
4. List of alternative solutions (protocols/algorithms/implementations) you are planning to explore:

- **AONT:**
  - Rivest AONT
  - Boyko’s AONT
  - Stinson’s AONT

- **Erasure code:**
  - Standard Reed-Solomon
  - Cauchy Reed-Solomon
  - Rabin's Information dispersal algorithm

5. Detailed description of problems/hypotheses you are planning to investigate:

- Researching on the security and implementation of AONT algorithms.
- Research on efficiency and implementation of erasure code algorithms

6. A tentative list of questions you will be seeking an answer to:

- Which AONT transformation is relatively more secure?
- Which erasure code algorithm is efficient?

7. Procedure for verifying the results of your investigation:

- Comparing results from previously verified case studies, online algorithm implementations, research papers, and scholarly papers.
- Relying on opinions of the experts.

8. Time schedule, including intermediate goals to be achieved by the dates of progress reports: *Oct. 15-17, Oct. 29-31, Nov. 12-14, Nov. 26-28:*

- From Oct. 15 to 17
  - Select algorithms from each type of transformation (Erasure Coding and AONT) and research on those topics.
  - Investigating past research in this area and presenting problems and recommended solutions.
- Overview of current technologies that are used for each component of distributed storage.
- Weekly group meetings
- Regular Meetings with Professor Gaj
- Weekly PowerPoint Presentations

- From Oct. 29 to 31
  - Comparison of each selected algorithms based on specific parameters such as performance, efficiency, and security.
  - Detailed presentation of proposed solutions and algorithms
  - Weekly group meetings
  - Regular Meetings with Professor Gaj
  - Weekly PowerPoint Presentations

- From Nov. 12 to 14
  - First draft of report
  - Weekly group meetings
  - Regular Meetings with Professor Gaj
  - Weekly PowerPoint Presentations

- From Nov 26 to 28
  - Future modification and upgradation field
  - Written Report to be ready by Nov 26
  - Weekly group meetings
  - Regular Meetings with Professor Gaj
  - Weekly PowerPoint Presentations
9. A list of possible areas, where the specification can change depending on the progress of the project:
   Checking execution time of the algorithms and comparing execution speed in different devices.

10. Tentative table of contents of your final report:
   1. Introduction
   2. Secure Distributed Storage components:
      a. AONT
         i. Rivest AONT
         ii. Boyko’s AONT
         iii. Stinson’s AONT
      b. Erasure codes
         i. Standard Reed-Solomon code
         ii. Reed-Solomon code
         iii. Rabin's Information dispersal Algorithm
   3. Comparison of Algorithms:
      a. AONT algorithm comparison
         i. Efficiency
         ii. Security
         iii. Ease of implementation
      b. Erasure Coding algorithm comparison
         i. Efficiency
   4. Future work
   5. Conclusion
   6. References

11. List of literature:


12. **Anything else you consider important:** N/A