Project Options & Grading

Students must choose one of the following project options, each with a different grading weight. Weekly deadlines begin this week, and adherence to the schedule is mandatory.

1. Write an article on Medium (80% of project marks)
    - The article must present a well-formed case study, subject to prior approval.
    - It should follow a structured format, include relevant references, and offer critical insights.
    - The quality of writing, depth of analysis, and engagement (e.g., comments or shares) will be considered.
2. Contribute to an existing GitHub repository (90% of project marks)
    - The contribution must be meaningful, such as adding a feature, or fixing a bug.
    - The repository owner must acknowledge the contribution.
    - Code quality, relevance, and impact on the project will be evaluated.
3. Conduct a structured research project (100% of project marks)
    - Complete a research paper following the provided weekly milestones given below in the document.
    - Use IEEE/ACM formatting and AI-powered tools for research and writing.
    - Meet all deadlines for topic selection, literature review, methodology, and final submission.
    - The grade will be determined based on the depth of research, critical analysis, and adherence to academic standards, with the goal of preparing the work for submission to a good ranking conference or a at least Q4 impact factor journal, subject to quality and standards.

Project Options & Collaboration

Students must choose one of the following project options, each with a different grading weight. Weekly deadlines begin this week, and adherence to the schedule is mandatory.

Different groups can collaborate by working on multiple project options within a similar topic. For example, one group may write a **Medium article**, another may contribute to a **GitHub repository**, and a third may conduct **structured research**—all focusing on a shared research theme in **Security in general, or an Interdisciplinary Domain**.

Additionally, groups may collaborate with individuals outside the course, such as researchers, developers, or industry professionals, to enhance the quality and impact of their work. However, all external contributions must be clearly acknowledged, and each student's role must be well-defined.

Authorship Requirement:

For any **publication, GitHub contribution, or publicly recognized work**, the **course instructor and teaching assistant (TA) will be listed as co-authors**. The instructor may also include **other contributors** at their discretion based on their involvement in the project.

Submission Format:

- **All submissions must be in LaTeX.**
- Research papers must follow the **IEEE/ACM LaTeX template** (preferably using Overleaf).
- GitHub contributions should include **well-documented LaTeX-based reports** where applicable.

Weekly Deadlines:

Please be reminded that all student groups for the upcoming project must be finalized no later than **September 14, 2025**. Once your team is confirmed, please ensure that you submit your project proposal by the assigned weekly deadlines. Adherence to this timeline is essential for planning and resource allocation, and no changes to group composition will be permitted after the stated date.

Article on Medium

Week 1: Topic Selection & Research

- Choose a topic relevant to **Security or an Interdisciplinary area**.
- Identify a niche or unique angle (e.g., **"Emerging AI-based Digital Forensics Techniques"** or **"IoT Security Threats in Smart Cities"**).
- Conduct preliminary research using **IEEE, ACM, Springer, or Elsevier** sources.
- Organize key references using **Zotero/Mendeley**.
- Outline 3-5 key questions your article will answer.

Deliverable: Finalized topic with key research questions.

Week 2: Structuring the Article

- Decide on the format: **Case Study, Thought Leadership, Technical Guide, or Comparative Analysis**.
- Create an outline with **an engaging introduction, key sections, and a strong conclusion**.
- List the references and real-world examples to include.
- Draft a rough **thesis statement** and main arguments.

Deliverable: Detailed article outline.

Week 3: Writing the Introduction & Background

- Hook the reader with a compelling **story, statistic, or recent cybersecurity event**.
- Explain why this topic matters in **industry, academia, or policy-making**.
- Provide historical context and define key terms.
- Write **1-2 pages** of a polished introduction.

Deliverable: Draft of the **Introduction & Background**.

Week 4: Core Content Development

- Write the **main sections**, breaking down complex ideas into **engaging, easy-to-read content**.
- Support claims with **research-backed evidence, real-world case studies, or expert opinions**.
- Ensure the content flows logically and **maintains reader engagement**.

Deliverable: First draft of **core content sections**.

Week 5: Data, Examples & Graphics

- Add **case studies, real-world examples, and technical insights**.
- Include **infographics, charts, or tables** (use tools like **Canva or Overleaf**).
- If relevant, demonstrate **hands-on techniques** (e.g., how to use Wireshark for digital forensics).
- Cite **high-impact research papers and industry reports**.

Deliverable: Enhanced draft with **data, case studies, and visuals**.

Week 6: Writing the Conclusion & Refining the Narrative

- Summarize key insights and **provide actionable takeaways**.
- Discuss **future directions or open challenges** in the field.
- Ensure the article **ends on a strong, thought-provoking note**.
- Strengthen transitions between sections for a **smooth reading experience**.

Deliverable: Draft of **conclusion & final structure refinement**.

Week 7: Editing, Proofreading & SEO Optimization

- Use **Grammarly, Hemingway Editor, and Wordtune** to improve clarity.
- Optimize for **SEO** (use relevant keywords for Medium’s algorithm).
- Refine **headlines, subheadings, and meta descriptions**.
- Get **peer feedback** or a mentor’s review before finalizing.

Deliverable: Final, polished article draft.

Week 8: Publishing & Promotion

- Publish on **Medium with engaging images, metadata, and hashtags**.
- Share on **LinkedIn, Twitter, and Reddit cybersecurity communities**.
- Engage with readers by **responding to comments and sharing insights**.
- Track **engagement metrics** and improve based on feedback.

Deliverable: Published Medium article + Engagement tracking.

Github Repository

Week 1: Identifying a Relevant GitHub Repository

- Explore open-source projects in **Security, or Interdisciplinary fields** on GitHub.
- Use **GitHub search, Awesome Lists, and curated repositories** to find active projects.
- Evaluate project relevance, community activity, and contribution guidelines.
- Engage with maintainers by introducing yourself in the discussions or issues.

Deliverable: Selected GitHub repository + understanding of its contribution process.

Week 2: Understanding the Codebase & Contribution Guidelines

- Fork the repository and set up the development environment.
- Review the **README, CONTRIBUTING.md, and past pull requests (PRs)**.
- Study the project's architecture, dependencies, and coding standards.
- Identify potential areas for contribution (**bug fixes, feature requests, documentation improvements**).

Deliverable: Familiarity with the codebase and a list of potential contribution ideas.

Week 3: Selecting a Contribution Task

- Choose a task aligned with your skills:
  - **Code contribution** (adding new features, fixing security vulnerabilities).
  - **Documentation improvement** (API documentation, installation guides, security best practices).
  - **Testing & debugging** (writing test cases, improving automation, fixing known issues).
- Discuss the contribution with maintainers (via GitHub Issues or Discussions).

Deliverable: Selected contribution task + approval from project maintainers.

Week 4: Development & Implementation

- Start working on the selected contribution.
- Follow project coding conventions and best practices.
- Write clean, well-documented, and maintainable code.
- If contributing documentation, ensure clarity, accuracy, and completeness.

Deliverable: Initial version of the contribution (code or documentation).

Week 5: Testing & Code Review

- Test your implementation thoroughly to ensure it meets project requirements.
- Run unit tests, security scans, and debugging tools where applicable.
- Address potential security concerns (especially for **network security and IoT contributions**).
- Refine and optimize your code based on test results.

Deliverable: Fully tested and debugged contribution ready for review.

Week 6: Submitting a Pull Request (PR)

- Create a **well-documented pull request (PR)** with:
  - A clear title and description.
  - A summary of changes and how they improve the project.
  - Any relevant screenshots or logs (for UI or security tools).
- Follow up with maintainers for feedback and iterate if necessary.

Deliverable: Successfully submitted **pull request (PR)** for review.

Week 7: Feedback & Final Adjustments

- Address **review comments** and make necessary modifications.
- Improve documentation or code readability if suggested.
- Engage in discussion with the community and maintainers.
- Resubmit changes and ensure the PR meets approval criteria.

Deliverable: Approved and merged **pull request (PR)**.

Week 8: Documentation, Reporting & Reflection

- Write a **contribution report**, summarizing:
  - What was contributed and its impact on the project.
  - Key challenges faced and how they were overcome.
  - Lessons learned from the process.
- Engage in post-merge discussions and look for further contribution opportunities.
- Share the experience on **LinkedIn, Medium, or GitHub Discussions**.

Deliverable: Final contribution report + public acknowledgment from project maintainers.

Structured Research

Select one of the following approaches:

1. **Experimental Study**
   - Conduct hands-on experiments, simulations, or prototype development.
   - Collect and analyze data using appropriate research methodologies.
   - Validate results through statistical or comparative analysis.
2. **Design Framework**
   - Develop a novel framework, model, or architecture addressing a research problem.
   - Provide theoretical justification and practical applications.
   - Compare with existing frameworks and demonstrate improvements.
3. **Survey Article or Systematic Review**
   - Conduct a **comprehensive literature review** using PRISMA or similar methodology.
   - Identify key trends, challenges, and future research directions.
   - Categorize studies based on methodology, contributions, and impact.
4. **Mixed-Method Survey**
   - Combine **quantitative and qualitative** research methods to analyze a problem.
   - Conduct surveys, interviews, or case studies for data collection.
   - Apply statistical techniques and thematic analysis to derive insights.

Annexure A includes a list of reference tools and websites designed to support your research process, covering literature review, citation management, writing assistance, and experimentation.

Week 1: Topic Selection & Research Question Formulation

- Choose a broad research area.
- Narrow it down to a **specific** focus (e.g., AI for ransomware detection).
- Define **research questions** (e.g., What are the latest AI-based ransomware detection methods?).
- Search for **10+ recent high-quality papers** (journals/conferences from IEEE, ACM, Springer, Elsevier, Q1/Q2/Q3/Q3 clarivate impact factor Journals and flagship conferences only).
- Organize papers in **Zotero / Mendeley**.

Deliverable: Research topic + 3-5 research questions

AI Tools: Semantic Scholar, Connected Papers, Elicit

Week 2: Literature Collection & Classification

- Collect 20+ relevant papers (published in the last 5 years).
- **Categorize papers** based on methodology, challenges, contributions.
- Create a comparative table (summarizing techniques, datasets, results).
- Identify key trends and research gaps.

Deliverable: Table summarizing key papers + research gaps

AI Tools: Scite, Research Rabbit, ChatGPT (for summarizing papers)

Week 3: Writing the Introduction & Background

- Explain why the selected area is important.
- Provide **historical context** (evolution of the field).
- Define key terms and concepts.
- Outline the scope of the paper (which aspects you cover and exclude).

Deliverable: 1-2 pages of Introduction & Background

AI Tools: Grammarly, QuillBot, Wordtune

Week 4: Writing the Literature Review

- Organize review **by themes** (e.g., "AI-based security techniques," "Forensic tools for IoT" or Interdisciplinary).
- Summarize each category with comparisons and critical insights.
- Highlight key research trends, challenges, and gaps.

Deliverable: 3-5 pages of literature review

AI Tools: ChatGPT (structured summarization), Elicit, Scholarcy

Week 5: Methodology (Survey Strategy)

- Explain how papers were **selected and classified** (e.g., PRISMA flowchart for systematic reviews, survey design, framework proposal, experimental study, or mathematical modeling).
- Justify inclusion/exclusion criteria.
- Describe how you analyzed and compared research works.

Deliverable: 1-page methodology section

AI Tools: Overleaf for PRISMA, Zotero for reference management

Week 6: Writing Discussion & Future Directions

- Discuss **current research trends** (What's dominant in recent papers?).
- Highlight **open challenges** (What are unsolved problems?).
- Propose **future research directions** (Where is the field heading?).

Deliverable: 2-3 pages of discussion & future work

AI Tools: AI-powered summarization (ChatGPT, QuillBot)

Week 7: Revision & Formatting

- Check citations and references.
- Ensure technical accuracy (reword vague claims).
- Format in **IEEE / ACM** style.
- Conduct **peer review** (exchange papers with classmates).

Deliverable: Full research paper draft

AI Tools: Turnitin (plagiarism check), Grammarly (proofreading)

Week 8: Final Submission & Presentation

- Make final edits and proofread.
- Prepare **presentation slides** (10-12 slides, 5-7 mins).
- Submit paper and slides.

Deliverables:
Final Research Paper (IEEE/ACM format)
Presentation slides (for in-class defense)

AI Tools: ChatGPT (slide summarization), Canva, PowerPoint

Annexure A

1. Topic Selection & Literature Review

Tool	Purpose	Notes
Connected Papers (https://www.connectedpapers.com)	Visualizes related papers & research trends	Helps students find relevant works
Semantic Scholar (https://www.semanticscholar.org)	AI-powered paper search engine	Summarizes key takeaways from papers
Elicit (https://elicit.org)	AI-assisted research tool	Finds and summarizes academic papers
Litmaps (https://www.litmaps.com)	Research mapping tool	Tracks citation relationships
Scite (https://scite.ai)	AI-based citation analysis	Shows how papers are cited in context

2. Writing & Drafting

Tool	Purpose	Notes
QuillBot (https://www.quillbot.com)	AI-powered paraphrasing & grammar checking	Helps with rewording and coherence
Grammarly (https://www.grammarly.com)	AI-driven grammar and clarity tool	Useful for improving sentence structure
Hemingway Editor (https://hemingwayapp.com)	Readability and conciseness checker	Highlights complex sentences
ChatGPT (GPT-4) (https://openai.com)	AI assistant for brainstorming & structuring text	Good for outlining and generating drafts
Wordtune (https://www.wordtune.com)	AI-based sentence rewriter	Improves clarity and tone

3. Citation Management & Formatting

Tool	Purpose	Notes
Zotero (https://www.zotero.org)	Citation management & bibliography generator	Supports IEEE, APA, and other formats
Mendeley (https://www.mendeley.com)	Reference manager with AI-based PDF annotation	Great for collaborative research
CiteThisForMe (https://www.citethisforme.com)	Quick citation generator	Helps format citations correctly

4. Plagiarism & Ethical Writing

Tool	Purpose	Notes
Turnitin (https://www.turnitin.com)	Plagiarism detection	Academic integrity tool
CrossPlag (https://www.crossplag.com)	AI-driven plagiarism checker	Alternative to Turnitin
Scribbr AI Paraphraser (https://www.scribbr.com)	Paraphrasing & citation assistance	Good for avoiding unintentional plagiarism

5. Experimentation & Simulation (for Practical Work)

Tool	Purpose	Notes
Metasploit (https://www.metasploit.com)	Penetration testing framework	Helps test security vulnerabilities
Wireshark (https://www.wireshark.org)	Network protocol analyzer	Useful for traffic analysis
NS3 (https://www.nsnam.org)	Network simulation tool	For modeling and testing network security scenarios
OpenVAS (https://www.openvas.org)	Vulnerability scanner	Helps evaluate security weaknesses