Table 1: Confusion matrix for mitre on attackVector

	N	**A**	**L**	**P**
N	0.41	0.19	0.2	0.19
A	0.2	0.4	0.2	0.21
L	0.2	0.19	0.41	0.2
P	0.2	0.21	0.2	0.39

Table 2: Confusion matrix for mitre on attackComplexity

	L	**H**
L	0.65	0.35
H	0.34	0.66

CVSS - Vulnerability Score Prediction
Supervisor(s): David Eyers Veronica Liesaputra

Aims The primary aim of this research is to develop sophisticated predictive models capable of accurately determining the severity levels of security threats based on the CVSS. This will involve a comprehensive review and comparison of current datasets, with a focus on leveraging natural language descriptions provided in security vulnerability reports. The project intends to utilize advanced transformer-based models to achieve this goal, contributing to the field of cybersecurity by enhancing the precision of threat severity assessments.

Objectives

Table 3: Confusion matrix for mitre on privilegesRequired

	N	**L**	**H**
N	0.5	0.25	0.25
L	0.24	0.52	0.24
H	0.25	0.26	0.5

Table 4: Confusion matrix for mitre on userInteraction

	N	**R**
N	0.66	0.34
R	0.33	0.67

Table 5: Confusion matrix for mitre on scope

	U	**C**
U	0.67	0.33
C	0.34	0.66

Table 6: Confusion matrix for mitre on confidentialityImpact

	N	**L**	**H**
N	0.5	0.24	0.27
L	0.24	0.5	0.26
H	0.25	0.25	0.5

Table 7: Confusion matrix for mitre on integrityImpact

	N	**L**	**H**
N	0.47	0.27	0.26
L	0.26	0.5	0.25
H	0.26	0.26	0.48

Table 8: Confusion matrix for mitre on availabilityImpact

	N	**L**	**H**
N	0.51	0.24	0.25
L	0.26	0.49	0.25
H	0.26	0.25	0.49

- Conduct a comprehensive literature review to understand the current landscape of CVSS score prediction and the methodologies employed in existing models.
- Replicate successful methodologies to verify the accuracy of CVSS score databases, with a particular focus on alignment with recent CVSS standards and datasets.
- Explore opportunities for enhancing existing methodologies, including the investigation of data amalgamation from multiple databases to ascertain improvements in model performance.
- Experiment with various model architectures to identify the most effective approach in terms of predictive accuracy, specifically focusing on metrics such as the F1 score and balanced accuracy.

Timeline

- March: Initiate the project with a literature review, system environment setup, and resource gathering.
- March-April: Replicate existing methodologies to validate findings and ensure alignment with current standards.
- May-June: Generate preliminary results and compile an interim report detailing findings and methodologies.
- July-August: Conduct experiments with various data source combinations and model architectures to identify optimal configurations.
- September-October: Finalize experimental work, analyze results, and prepare the comprehensive final report.