

LIST OF FIGURES

2.1	Concept of n-Gram	7
3.1	Study Design for the Proposed Method	19
3.2	Dataset Construction and Feature Extraction Flowchart	20
3.3	Architecture of the Proposed Response Time Detection Model	21
4.1	Response Time Detection Results on WannaCry Test Data Using Naive Bayes and 10-Gram	22
4.2	Response Time Detection Results on LockBit Test Data Using Naive Bayes and 10-Gram	22
4.3	Learning Curve Naive Bayes 8-gram	23
4.4	Learning Curve Naive Bayes 10-gram	24
4.5	Evaluation of Naive Bayes Performance on the API Call Ransomware Dataset Response Time Detection with Delayed Window 0-80,000 API Calls.	31
4.6	Evaluation of Random Forest Performance on the API Call Ransomware Dataset Response Time Detection with Delayed Window 0-80,000 API Calls.	32
4.7	Evaluation of Support Vector Machine Performance on the API Call Ransomware Dataset Response Time Detection with Delayed Window 0-80,000 API Calls.	32
4.8	Evaluation of Naive Bayes Model Performance on the System Call Ransomware Dataset (DIB and DABRI 2022) with Delayed Window 0-80,000 System Calls.	34
4.9	Evaluation of Random Forest Model Performance on the System Call Ransomware Dataset (DIB and DABRI 2022) with Delayed Window 0-80,000 System Calls.	35
4.10	Evaluation of Support Vector Machine Model Performance on the System Call Ransomware Dataset (DIB and DABRI 2022) with Delayed Window 0-80,000 System Calls.	35
4.11	Execution Phases of Normal Programs Based on API Call Analysis	38
4.12	Analysis of Unique API Calls Over Time in Normal Execution, Showing Different Operational Phases	38
4.13	Execution Phases of Ransomware Based on API Call Analysis	41
4.14	Analysis of Unique API Calls Over Time in Ransomware Execution, Showing Different Phases of Malicious Behavior	41
4.15	Effect of n-grams on Execution Time and Data Size	43
4.16	Comparison of Cumulative API Calls Over Time for Normal and Ransomware Samples	43