|  |
| --- |
| **CONTENTS** |
|  |
| |  |  | | --- | --- | | **Chapter** | **Page no** | | **1. Introduction**   1. Various IDS 2. Network IDS 3. Host IDS 4. Anomaly based IDS 5. Signature based IDS 6. Application protocol based IDS 7. Function of IDS | **1**  2  2  3  3  3  4  4 | | **2. Problem Statement**   * + 1. Existing System  1. Issues in existing IDS    * 1. Proposed System 2. Integrating LIDS with conditional random field | **5**  5  5  6  6 | | **3. Literature Survey**   1. A detailed analysis of the KDD CUP 99 data set 2. Syntax & semantics-based signature database for hybrid   IDS   1. Intrusion detection using data mining techniques | **8**  8  9  9 | | **4. Requirements Specifications** | **12** | | **5. System Analysis**   1. Approaches for IDS 2. Pattern matching 3. Statistical methods 4. Machine learning 5. Clustering 6. Data mining 7. Bayesian classifiers 8. Decision trees 9. Project Description 10. Challenges and requirements for IDS 11. Conditional Random Fields 12. Manual Feature Choice 13. DOS attacks 14. Probe attacks 15. R2L attacks 16. U2R attacks 17. Framework of stratified approach   5.6.1 WinPcap  5.6.2 Preprocessor  5.6.3 Signature database  5.6.4 Detection engine   1. Building individual layers 2. Algorithm And Training | **15**  15  15  15  16  16  16  16  17  17  18  19  20  21  21  21  21  21  23  23  23  24  25  25 | | **6. System Design**   1. Dataflow Diagrams 2. UML Diagrams   6.2.1 Use Case Diagram  6.2.2 Sequence Diagram | **28**  28  31  31  32 | | **7. Implementation** | **33** | | **8. Testing**   1. Test cases | **35**  35 | | **9. Result Screens** | **37** | | **Conclusion** | **42** | | **References** | **43** | | **APPENDIX** |  | |