TABLE OF CONTENTS

1. Introduction 1

1.1 Data Exfiltration Method 1

2. Literature Survey 2-11

2.1 Anomaly Detection Overview 2

2.1.1 Detailed Survey of Anomaly Detection 2-7

2.1.1.1 Network Based Anomaly Detection 2-4

2.1.1.2 Host Based Anomaly Detection 5-7

2.2 Covert Channel Overview 8

2.2.1 Detailed Survey of Covert Channel 8-11

2.1.1.1 Covert Communication 8-9

2.1.1.2 Covert Channel With Wireless Network 9-11

3. Work Summery 12

4. Proposed Algorithm 12-13

5. Related Work Model 14-15

5.1 Key Concerns Of Insider Attack 14

5.2 Related Work 14

5.3 Model 14-15

5.3 References 15

6. System Design 16

6.1 Introduction 16

6.2 Database Design 16

7. UML Design 17

8. Experimental Results

And Analysis 18-19

8.1 Learning Phase 18

8.2 Detection Phase 19

9. Implementation 20

10. Conclusion 21