# INTRUSION DETECTION AND ITS HASHING TECHNIQUES

Submitted in partial fulfillment of the requirements for

the award of

Bachelor of Engineering degree in Computer Science and Engineering

by

K.PADMA PRIYANKA(36110873)

O. APARNA(36110867)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SCHOOL OF COMPUTING**

**SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**

### (DEEMED TO BE UNIVERSITY)

**Accredited with Grade “A” by NAAC**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,**

**CHENNAI - 600 119**

### MARCH - 2020

**SATHYABAMA**

INSTITUTE OF SCIENCE AND TECHNOLOGY

# (DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

**[www.sathyabama.ac.in](http://www.sathyabama.ac.in/)**

# DEPARTMENT OF

**BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work of **KUNCHAM PADMA PRIYANKA(36110873)** who have done the Project work as a team **kuncham padma priyanka (36110873) ,Obilineni aparna (36110867)** who carried out the project entitled **“INSTRUSION DETECTION AND ITS HASHING TECHNIQUES”** under my supervision from **NOVEMBER 2019** to **APRIL 2020**.

**Internal Guide**

Dr.A.CHRISTY M.C.A.,Ph.D,

# Head of the Department

**Submitted for Viva voce Examination held on**

**Internal Examiner** **External Examiner**

# DECLARATION

I Kuncham padma priyanka hereby declare that the Project Report entitled **“INTRUSION DETECTION AND ITS HASHING TECHNIQUES”** done by me under the guidance of **Dr.A.CHRISTY M.C.A.,Ph.D.,**is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering in computer science and engineering .

**DATE**

**PLACE SIGNATURE OF THE CANDIDATE**

# ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D**, **Dean**, School of Computing , **Dr.S.Vigneshwari M.E., Ph.D. and Dr.L.Lakshmanan M.E., Ph.D. , Heads** of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.A.Christy M.C.A.,Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

**ABSTRACT**

Today data sharing and maintaining its security is major challenge. User in the data sharing system upload their file with the encryption using private key. This property is especially important to any large scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this project, we provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This project will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using RSA Encryption Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority send file to cloud service provider module to store on cloud.The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes.

**TABLE OF CONTENTS**

**CHAPTER NO. TITLE. PAGE NO.**

**ABSTRACT v**

**LIST OF FIGURES IX**

**LIST OF TABLES X**

**LIST OF ABBERIVATIONS XI**

1. **INTRODUCTION 1**

1.1 DOMAIN 1

1.2 AIM AND OBJECTIVE 1

1.2.1 CHARACTERISTICS 1

1.3 EXISTING SYSTEM 1

1.3.1 DISADVANTAGES OF EXIXTING

SYSTEM 2

1.4 PROPOSED SYSTEM 2

1.4.1 ADVANTAGES OF PROPOSED

SYSTEM 2

1. **LITERATURE SURVEY 3**
2. **MATERIALS,METHOD AND ALGORITHUM USED 6**

3.1 SYSTEM REQUIREMENTS 6

3.1.1 HARDWARE REQUIREMENTS 6

3.1.2 SOFTWARE REQUIREMENTS 6

3.2 SYSTEM ARCHITECTURE 6

3.3 LANGUAGE OVERVIEW 7

3.3.1 INTRODUCTION TO JAVA 7

3.3.2 APPLICATIONS OF JAVA 7

3.3.3 FEATURES OF JAVA 7

3.4 MY SQL 9

3.5 NETBEANS 9

3.6 JAVA NETWORKING 9

3.7 REQUIREMENT ANALYSIS 9

3.8 FUNCTIONAL REQUIREMENTS 10

3.9 MODULES 11

3.9.1 LOGIN MODULE 11

3.9.2 REGISTRATION MODULE 12

3.9.3 FILE UPLOAD MODULE 12

# 3.9.4 INTRUSION DETECTION MODULE 13

3.9.5 DETECT INTRUDER MODULE 13

3.10 DATA FLOW DIAGRAM 13

3.11 SYSTEN DESIGN 15

3.11.1 INPUT DESIGN 15

3.11.2 OUTPUT DESIGN 15

3.12 PROPOSED ALGORITHM 15

3.12.1 RSA ENCRYPTION 15

3.12.2 THE BOOTSTRAP PROCESS 16

3.12.3 MD5 ALGORITHM 17

3.12.4 SHA ALGORITHM 19

**4 RESULT AND DISCUSSION 21**

4.1 SYSTEM TESTING 21

4.1.1 TESTING PROCESS 21

4.2 TYPES OF TESTS 21

4.2.1 UNIT TESTING 21

4.2.2 INTEGRATION TESTING 21

4.2.3 FUNCTIONAL TESTING 22

4.2.4 TEST STRATEGY AND APPROACH 23

4.2.5 ACCEPTANCE TESTING 23

4.2.6 ALPHA TESTING 23

4.2.7 BETA TESTING 23

**5 CONCLUSION AND FUTURE WORK 25**

**REFERENCES 26**

**APPENDIX 27**

**A .SOURCE CODE 28**

1. **SCREENSHOTS 57**

|  |  |  |
| --- | --- | --- |
|  | B.1 File download page | 57 |
|  | B.2 File upload page | 58 |
|  | B.3 Intuder detection page | 58 |
|  | B.4 Intrusion detection page | 59 |
|  | B.5 login page | 59 |
|  | B.6 admin page | 59 |
|  | B.7 group name registration page | 60 |
|  | B.8 user registration page | 60 |
|  | B.9 file deletion page  **PAPER** | 61 |
|  |  |  |

**LIST OF FIGURES**

**FIGURE NO.** **FIGURE NAME** **PAGE NO.**

3.1 Architecture of system module 6

3.2 Login Module 11

3.3 Registration Module 12

3.4 File Upload Module 12

3.5 Intrusion detection Module 13

3.6 Detect Intruder Module 13

3.7 DFD-Level 0- Data Owner 14

3.8 DFD-Level 1 14

3.9 DFD-Level 2 14

3.10 Auxiliary function 18

4.1 Unit Testing 21

4.2 graph 29

**LIST OF TABLES**

**TABLE NO. TITLE PAGE NO.**

3.1  key self-mutating 17

**LIST OF ABBERIVATIONS**

**ABBERIVATION EXPANSION**

RSA  Rivest–Shamir–Adleman

MD5 Message-digest

SHA Secure hash algorithum