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

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

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBERIVATIONS

ABBERIVATION	EXPANSION
RSA	Rivest–Shamir–Adleman
MD5	Message-digest
SHA	Secure hash algorithum