VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI



PROJECT REPORT ON

EFFICIENT MESSAGE TRANSMISSION USING HYBRID CRYPTOGRAPHY

Submitted in partial fulfilment of the award of degree in

BACHELOR OF ENGINEERING

In

INFORMATION SCIENCE & ENGINEERING

By

CHANDANA PT 4AL20IS011

KEERTHANA G 4AL20IS020

SHWETHA R SHARMA 4AL20IS047

SWETHA S 4AL20IS054

Under the Guidance of

Prof. Jayantkumar A Rathod

Associate Professor



DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY MOODBIDRI-574225, KARNATAKA 2023 – 2024

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY MIJAR, MOODBIDRI-574225



DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the Project work entitled "EFFICIENT MESSAGE TRANSMISSION USING HYBRID CRYPTOGRAPHY" has been successfully completed by

CHANDANA PT

4AL20IS011

KEERTHANA G

4AL20IS020

SHWETHAR SHARMA

4AL20IS047

SWETHAS

4A1,20IS054

the Bonafide students of Information Science & Engineering Department, Alva's Institute of Engineering and Technology, Moodbidire, in partial fulfilment of 8th Semester BACHELOR OF ENGINEERING, affiliated to VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI, during the year 2023-2024. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the Bachelor of Engineering Degree.

H. O. D.

Prof. Jayantkumar A Rathod Dept. Of InDrataidh Suichte LyEngineering Dr.

Alva's Institute of Engg. & Technology Mijar, MOODBIDRI - 574 225 HOD ISE

PraRINGIPAL

Alve's Institute of Engg. & Technology,

Peter Fernandes

Mijar. MOODBIDRI - 574 225, D.K.

EXTERNAL VIVA

Name of the Examiners

Associate Professor

Guide

Signature with Date

1. Dr. Sudheed Slety 2. Dr. Rittsch Paucele

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY MIJAR, MOODBIDRI-574225



DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING DECLARATION

We,

CHANDANA PT

KEERTHANA G

SHWETHA R SHARMA

SWETHAS

hereby declare that the dissertation entitled, EFFICIENT MESSAGE TRANSMISSION USING HYBRID CRYPTOGRAPHY is completed and written by us under the supervision of our guide Prof. Jayantkumar A Rathod, Associate Professor, Department of Information Science and Engineering, Alva's Institute of Engineering and Technology, Moodbidri, in partial fulfilment of the requirements for the award of the degree BACHELOR OF ENGINEERING in DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING of the VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI during the academic year 2023-2024. The project report is original and it has not been submitted for any other degree in any university.

CHANDANA P T

4AL20IS011

KEERTHANA G

4AL20IS020

SHWETHAR SHARMA

4AL20IS047

SWETHAS

4AL20IS054

ABSTRACT

Our system introduces a novel approach to secure data transmission, harnessing the combined strengths of RSA and Blowfish encryption algorithms. By employing RSA for secure key exchange and Blowfish for efficient data packet encryption, we aim to enhance data transmission security while minimizing the risk of unauthorized access on wireless networks. Our approach offers reduced data exposure and potentially lower network overhead compared to conventional methods like selective or full encryption. Furthermore, we consider various performance parameters such as delay, energy efficiency, consumption, and packet delivery ratio to comprehensively assess the effectiveness of our security measures.

We also consider factors like delay, energy use, and packet delivery rate to gauge how well our security measures work. We emphasize that only the intended recipient can decode the encrypted data, keeping it confidential. We use algorithms that add uncertainty to the encryption process, so unauthorized users can't understand the communication. We emphasize the importance of confidentiality, ensuring that only the intended recipient can decipher the ciphertext. To enhance security, we utilize probabilistic algorithms to introduce uncertainty into the encryption process, thwarting unauthorized access. Additionally, our system incorporates authentication, access control, and integrity checks to further fortify its security.

The effectiveness of our selected algorithms and security mechanisms is validated through extensive simulation studies using the NS2 simulator. These simulations provide valuable insights into the real-world applicability and robustness of our proposed secure data transmission solution, offering a comprehensive understanding of its performance under diverse scenarios and conditions.

ACKNOWLEDGMENT

The satisfaction and euphoria that accompany a successful completion of any task would be incomplete without the mention of people who made it possible, success is the epitome of hard work and perseverance, but steadfast of all is encouraging guidance.

So, with gratitude we acknowledge all those whose guidance and encouragement served as beacon of light and crowned the effort with success.

The selection of this Synopsis as well as the timely completion is mainly due to the interest and persuasion of our Project guide Prof. JAYANTKUMAR A RATHOD, Associate Professor, Department of Information Science & Engineering. We will remember his contribution forever.

We thank our beloved Project coordinator Prof. JAYANTKUMAR A RATHOD, for his constant help and support throughout.

We sincerely thank **Dr. SUDHEER SHETTY**, Professor and Head, Department of Information Science & Engineering who has been the constant driving force behind the completion of the project.

We thank our beloved Principal Dr. PETER FERNANDES, for his constant help and support throughout.

We are indebted to Management of Alva's Institute of Engineering and Technology, Mijar, Moodbidire for providing an environment which helped us in completing our Synopsis.

Also, we thank all the teaching and non-teaching staff of the Department of Information Science & Engineering for the help rendered.

CHANDANA P T 4AL20IS011

KEERTHANA G 4AL20IS020

SHWETHA R SHARMA 4AL20IS047

SWETHA S 4AL20IS054

CONTENTS

Chapter	Description	Page
no.		no.
	CERTIFICATE	PAGE NO.
	DECLARATION	10 II
	ABSTRACT	***
	ACKNOWLEDGMENT	IV
	TABLE OF CONTENT	v
	LIST OF FIGURES	VI
	LIST OF TABLES	VII
1	INTRODUCTION	1
2	LITERATURE SURVEY	2-4
3	PROBLEM DEFINITION AND OBJECTIVES	5-6
	2 1 DDODY ENG COLUMN	5
	3.2 OBJECTIVE	6
4	METHODOLOGY	7-11
	4.1 PACKET DELIVERY RATIO	7
	4.2 DELAY	8
	4.3 ENERGY EFFICIENCY	8
	4.4 ENERGY CONSUMPTION	8-9
	4.5 RESIDUAL ENERGY	9
	4.6 FLOW OF CONCEPT	9-11
5	SYSTEM REQUIREMENT SPECIFICATION	12-16
	5.1 HARDWARE SPECIFICATION	12
	5.2 SOFTWARE SPECIFICATION	12-15
	5.3 STRUCTURE OF NS2	15-16
6	SYSTEM ARCHITECTURE AND DESIGN	17-21
	6.1 EXISTING SYSTEM	17
	6.2 PROPOSED SYSTEM	17-19
	6.3 ALGORITHMS	19-21
7 7.98	RESULTS AND DISCUSSIONS	22-39
8	CONCLUSION	40
	REFERENCES	41-42

LIST OF FIGURES

FIGURE NO.	NAME	PAGE NO.
4.1	Flow diagram of the concept	10
6.1	Block Diagram of proposed system	7 8 2 18
7.1	Fragmentation calculation	23
7.2	Source and Destination selection	24
7.3	RSA Encrypted packet transmission	25
7.4	Blowfish Encrypted packet transmission	26 & 27
7.5	Blowfish encrypted packets	28
7.6	RSA Encrypted packets	29
7.7	Performance of the proposed system	30
7.8	Energy performance of the system	31
7.9	PDR graph	32
7.10	Delay graph	33
7.11	Energy efficiency graph	34
7.12	Consumption graph	35
7.13	Residual energy graph	36
7.14	Comparison graph of PDR's	37
7.15	Delay graph	38
7.16	Energy graph	39

LIST OF TABLES

Table no.	Name	Page no.
5.1	Simulation parameters	14

INTRODUCTION

The Table Sales of the Sales of

to an animal angular point their a mustile extended of makes are considered the performance of the second and animal transfer that the contrast transfer the contrast transfer the animals increased attending requirements, for example, originariasis and the contrast of animals animals are particularly common today to a contrast or an animal typological companies beginning to the animals are not a contrast to the animals of the animals and the animals are not transfer to the animals and the animals are not transfer to the animals and the second transfer to the animals and the animals are animals and the animals and the animals are animals and the animals and the animals are animals and the animals are animals and animals.

INTRODUCTION

some consistent in a marger catalletings in sciences, and mobile accounts.

As a constituent of factors a subscipul operation recharges anglet dramatically reduce unreless, developed account of processing time and processing time and

the course of the enterior of the enterprise traces. Our printary goal is use done private formats and is use done provide the course of the enterior of the e

the control operation of the matter of the control of the control

The committee of the state of the second data from the second second second of the second second sections the committee of the second sections the committee of the second sections are second second sections.