SECURING USER DATA IN CLOUD USING ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

A PROJECT REPORT

Submitted by

B DHINESHA	**611420104017**
M MAHALAKSHMI	**611420104035**
G PRIYA	**611420104058**
G VINODHA	**611420104094**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

MAHENDRA ENGINEERING COLLEGE FOR WOMEN
TIRUCHENGODE, NAMAKKAL-637205

ANNA UNIVERSITY: CHENNAI 600 025

JUNE 2023

ANNAUNIVERSITY CHENNAI-600 025

BONAFIDE CERTIFICATE

Certified that this at project report "**SECURING USER DATA IN CLOUD USING ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM"** is the bonafide work of "**B.DHINESHA (611420104017),M.MAHALAKSHMI (611420104035), G.PRIYA (611420104058)**and **G.VINODHA (611420104094)"** who carried out the project work under my supervision.

SIGNATURE	**SIGNATURE**
Dr.A. KANCHANA, M.E., Ph.D.,	**Ms. M. GOMATHI, M.E.,**
HEAD OF THE DEPARTMENT	**SUPERVISOR**
	ASSISTANT PROFESSOR
Department of Computer Science and Engineering, Mahendra Engineering College for Women, Tiruchengode-637205.	Department of Computer Science and Engineering, Mahendra Engineering College for Women, Tiruchengode-637205.

Submitted for the University Project Viva-Voce held on ____________

INTERNAL EXAMINAR EXTERNAL EXAMINAR

ACKNOWLEDGEMENT

We would like to take this opportunity to say our thanks to the people who have helped us to make this project a reality.

We wish to express our honorable thanks to our beloved **Chairman Shri. M.G.BHARATHKUMAR, M. A, B.Ed., M.I.S.T.E.,** Mahendra Educational Trust and the Managing Directors **Mr. Ba. MAHENDRAN, B.E., M.I.S.T.E.,** and M**r. Ba. MAHA AJAY PRASAD, B.E., M.S., M.I.S.T.E.,** providing an extraordinary infrastructure.

We are highly obliged to **Dr. B.DORA ARULSELVI,M.E,ph.D., principal** of Mahendra Engineering College for Women, for giving us such an excellent opportunity to do this project work.

We also thanks to **Dr. A. KANCHANA, M.E., Ph.D., Head of the Department,** and **Mr. M. SARAVANAN, M.E., Assistant Professor,** our internal guide. Department of Computer Science and Engineering for her encouragement valuable suggestions and support in doing this project.

We would like to say our sincere thanks to all other faculties. Department of Computer Science and Engineering for their active and Kind guidance and advices for our project.

Above all we would like to express our sincere thanks and gratitude to our parents and friends for their valuable comments and suggestion for making this work a success.

ABSTRACT

Cloud is an emerging technology utilized by various fields for storage purpose and accessing it from anywhere at any time. Based on amount of storage utilization user can buy storage that is flexible and efficient. Cloud application and its usage are enhancing day by day and more number of research works is processing in security factor. Cloud is Honest but Curious hence user should ensure their data is in protected for this different encryption algorithms are available and individually each has its level of protection.

The need of encryption in cloud is attacker's different types of attacks are available to hack user data in cloud storage. In proposed work, user needs to utilize cloud facilities at the same time their data should be protected. To achieve this owner's data are encrypted using Elliptic curve cryptograph (ECC) and stored in cloud. Data user who needs the file is initially authorized and verified then downloads it in encrypted form. Once decryption key of ECC is received by receiver is used to decrypt that particular file. Compared to other encryption algorithm ECC provides high level of security and it explained clearly in proposed work.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No.
	ABSTRACT	**iv**
	LIST OF FIGURES	**viii**
	LIST OF ABBREVIATIONS	**ix**
1	**INTRODUCTION**	**1**
	1.1 CLOUD COMPUTING	1
	1.1.1 Cloud Data Storage Challenges &amp; Issues	1
	1.1.2 Cloud Storage issues	1
	1.1.3 Identity Management and Access Control	2
	1.1.3.1 Malicious insiders	2
	1.1.3.2 Outside intruder	2
	1.2 ELLIPTIC CURVE CRYPTOGRAPHY	2
2	**LITERATURE SURVEY**	**3**
3	**SYSTEM ANALYSIS**	**6**
	3.1 EXISTING SYSTEM	6
	3.1.1 Disadvantages	6
	3.2 PROPOSED SYSTEM	6
	3.2.1 Advantages	7
4	**SYSTEM STUDY**	**8**
	4.1 FEASIBILITY STUDY	8
	4.1.1 Economical feasibility	8
	4.1.2 Technical feasibility	8
	4.1.3 Social feasibility	9

5	**SYSTEM REQUIREMENTS**	**10**
	5.1 HARDWARE REQUIREMETS (Minimum requirement)	10
	5.2 SOFTWARE REQUIREMENTS	10
6	**SOFTWARE ENVIRONMENT**	**11**
	6.1 INTRODUCTION TO FROND END	11
	6.1.1 User interface	11
	6.1.2 Java	11
	6.1.3 The java platform	12
	6.1.4 Networking basics	13
	6.1.5 Socket overview	13
	6.1.6 Client/Server	13
	6.1.7 Reserved sockets	14
	6.1.8 Java and the net	14
	6.1.9 Inet address	14
	6.1.9.1 Factory methods	14
	6.1.10 Instance methods	15
	6.1.11 Tcp/Ip client sockets	15
	6.1.12 Tcp/Ip server sockets	15
	6.2 INTRODUCTION TO BACK END	16
	6.2.1 Microsoft sql server 2005	16
	6.2.2 Windows 2005 and sql server security	16
	6.2.3 Active directory users and groups	16
	6.2.4 Sql server logins	17
	6.2.5 Database roles	17
	6.2.6 Database user account	17
7	**SYSTEM DESIGN**	**19**
8	**SYSTEM TESTING**	**20**
	8.1 TYPES OF TESTS	20
	8.1.1 Unit testing	20

	8.1.2 Integration testing	20
	8.1.3 Functional test	20
	8.1.4 System test	21
	8.1.5 White box testing	21
	8.1.6 Black box testing	21
	8.2 UNIT TESTING	21
	8.2.1 Test strategy and approach	21
	8.2.2 Test objectives	21
	8.2.3 Features to be tested	22
	8.3 INTEGRATION TESTING	22
	8.3.1 Test results	22
	8.4 ACCEPTANCE TESTING	22
	8.4.1 Test results	22
9	**IMPLEMENTATION**	**23**
	9.1 PROPOSED SECURITY SOLUTION	23
	9.1.1 Elliptic curve cryptography domain parameters	24
10	**INPUT AND OUTPUT DESIGN**	**26**
	10.1 INPUT DESIGN	26
	10.2 OBJECTIVES	26
	10.3 OUTPUT DESIGN	26
	10.3.1 Database design	27
	10.3.2 Code design	27
11	**CONCLUSION**	**28**
	APPENDICES	
	APPENDIX 1	29
	SOURCE CODE	
	APPENDIX 2	56
	SCREENSHOTS	
	REFERENCES	59

LIST OF FIGURES

FIGURE No.	FIGURE NAME	PAGE No.
1.1	REGISTRATION PAGE	56
1.2	LOGIN PAGE	56
1.3	GENERATE PRIVATE AND PUBLIC KEY	57
1.4	SEND REQUEST	57
1.5	ACCEPT REQUEST	58
1.6	DATA RECEIVED	58

LIST OF ABBREVIATIONS

GUI	Graphical User Interface
CSPs	Cloud Service Provider
XML	Extensible Markup Language
IP	Internet programming
ECC	Elliptic Curve Cryptography
CPU	Central Processing Unit
OTP	One-Time Password
DBMS	Database Management System
TCP	Transmission Control Protocol
API	Application Protocol Interface
UDP	User Datagram Protocol
RMI	Remote Method Invocation
HTTP	Hyper Text Transfer Protocol
DTS	Data Transformation services
SQL	Structured Query Language
AWT	Abstract Window Toolkit
URL	Uniform Resource Locator
OLE	Object Linking And Embedding
Unix	Uniplexed Information Computer System