**ABSTRACT**

Distributed Mobile Computing is a technology, used to access resources, files and some other user data. But the Distributed System is not a trusted one because there are many organizations that provide many services in this environment and there are many semi trusted third parties that provide this technology to develop some business and use the resources like platform, application, storage etc. So, the user file needs security from the third party system and other intruders in the network. The proposed method aimed to solve this user needs by adding variant security to the user files and then the file is shared by the user to the third party system, whenever the user wants the file it can be downloaded from the third party system and easily use the files which is uploaded by the user. This system takes the valuable data as a input and then apply the cryptographic algorithms such as AES, Blowfish, RC4 to secure the information and the algorithms are used in a random manner that means every time it changes its pattern for encryption the pattern is again deployed by the system in reverse to recover the information. Finally the system provides data integrity, data authentication, data privacy and flexible data distribution with access controlto the organization or some other users who are using this system.

**TABLE OF CONTENTS**

**CHAPTER NO TITLE PAGE NO**

ABSTRACT i

LIST OF TABLES ii

LIST OF FIGURES iii

LIST OF ABBREVIATIONS iv

1. INTRODUCTION 1

1.1 OBJECTIVE OF THE PROJECT 2

1.2  LITERATURE SURVEY 2

1.3 OVERVIEW 5

1.4 SCOPE OF THE PROJECT 7

2 EXISTING SYSTEM 7

3 PROPOSED SYSTEM 8

3.1 ALGORITHM 10

3.1.1 ADVANCED ENCRYPTION STANDARD 10

3.1.2 RC 13

3.1.3 BLOWFISH 15

3.1.4 RANDOM FUNCTION 18

4 SYSTEM ORGANIZATION 20

4.1 SYSTEM ARCHITECTURE 20

4.1.1 ENCRYPTION 20

4.1.2 DECRYPTION 21

4.2 SYSTEM REQUIREMENTS 22

4.2.1 HARDWARE REQUIREMENTS 22

4.2.2 SOFTWARE REQUIREMENTS 22

5 SYSTEM ANALYSIS 22

5.1 MODULES 22

5.2 MODULES DESCRIPTION 23

5.2.1 START 23

5.2.2 NAVIGATOR 23

5.2.3 ENCRYPTION 24

5.2.4 DECRYPTION 25

5.2.5 UPLOAD 26

5.2.6 DOWNLOAD 27

5.3 DATA FLOW DIAGRAM 27

5.3.1 PROCESS 28

5.3.2 DATA STORES 29

5.3.3 EXTERNAL ENTITIES 29

5.3.4 DATA FLOWS 29

5.4 UML DIAGRAMS 32

5.4.1 USE CASE DIAGRAM 33

5.4.2 CLASS DIAGRAM 34

5.4.3 SEQUENCE DIAGRAM 35

5.4.4 ACTIVITY DIAGRAM 36

5.5 OUTPUT SEREENSHOTS 37

5.5.1 INTRODUCTION 37

5.5.2 NAVIGATOR 37

5.5.3 ENCRYPTION 38

5.5.4 DECRYPTION 40

5.5.5 UPLOAD 43

5.6 SAMPLE CODING 46

6 CONCLUSION AND FUTURE WORK 48

REFERENCE 49

PUBLICATION DETAILS 53

**LIST OF TABLES**

**Table NO TITTLE PAGE NO**

3.1.2 RC4 COMPARISON TABLE 14

**LIST OF FIGURES**

**FIGURE NO TITTLE PAGE NO**

3.1.1 AES DATA STRUCTURE 10

3.1.1a INPUT AND OUTPUT 11

3.1.1b KEY AND EXPANDED KEY 11

3.1.2 RC4 STREAM GENERATION 13

3.1.3 BLOWFISH STRUCTURE 15

3.1.4 RANDOM FUNCTION 18

4.1.1 ENCRYPTION 19

4.1.2 DECRYPTION 20

5.2.1 STARTUP MODULE 21

5.2.2 NAVIGATOR MODULE 22

5.2.3 ENCRYPTION MODULE 23

5.2.4 DECRYPTION MODULE 24

5.2.5 UPLOAD MODULE 25

5.3 LEVEL 0 DATA FLOW DIAGRAM 28

5.3 LEVEL 1 DATA FLOW DIAGRAM 28

5.3 LEVEL 2 DATA FLOW DIAGRAM 29

5.4.1 USE CASE DIAGRAM 31

5.4.2 CLASS DIAGRAM 32

5.4.3 SEQUENCE DIAGRAM 33

5.4.4 ACTIVITY DIAGRAM 34

5.5.1 INTRODUCTION 37

5.5.2 NAVIGATOR 37

5.5.3.1 ENCRYPTION 38

5.5.3.2 MODULE WITH DATA 38

5.5.3.3 MODULE WITHOUT DATA 39

5.5.3.4 FILE ENCRYPTED 39

5.5.4.1 DECRYPTION 40

5.5.4.2 DIALOUGE WITH USER 40

5.5.4.3 FILE EXPLORER 41

5.5.4.4 MODULE WITHOUT DATA 41

5.5.4.5 MODULE WITH DATA 42

5.5.5.1 UPLOAD 43

5.5.5.2 FILE EXPLORER 43

5.5.5.3 WITHOUT FILE 44

5.5.5.4 WITH FILE 44

5.5.5.5 FILE UPLOADING 45

5.5.5.6 FILE UPLOADED 45

**LIST OF ABBREVIATIONS**

**ABBREVATION EXPANSION**

AES Advanced Encryption Standards

RC4 Rivest Cipher 4

DFD Data Flow Diagram

UML Unified Modeling Language

USB Universal Serial Bus