**PROVIDING FILE SECURITY IN PUBLIC CLOUD INFRASTRUCTURE**

**A PROJECT REPORT**

|  |
| --- |
| ***Submitted by*** |
| **VINOTH KUMAR J.G** |
| **ULAGAPANDI U** |
| **UMAI ORU BAGAM V** |
| **VINOTH K** |

***in partial fulfilment of the award of the degree***

***of***

**BACHELOR OF ENGINEERING**

***in***

**COMPUTER SCIENCE AND ENGINEERING**

**PSNA COLLEGE OF ENGINEERING AND TECHNOLOGY,**

**DINDIGUL**

****

**ANNA UNIVERSITY: CHENNAI 600 025**

**APRIL 2018**

**ANNA UNIVERSITY: CHENNAI 600025**

**BONAFIDE CERTIFICATE**

Certified that the project report “**PROVIDING FILE SECURITY IN PUBLIC CLOUD INFRASTRUCTURE**” is the bonafide work of “**J.G.VINOTHKUMAR (921314104248), U.ULAGAPANDI (921314104223), K.VINOTH (921314104247), V.UMAI ORU BAGAM (921314104225)**” who carried out the project under my supervision.

**SIGNATURE**

**SIGNATURE**

**Dr. D.SHANTHI., M.E, Ph.D.**

**Mr. R.KARTHIKEYAN., M.Tech.,**

**HEAD OF THE DEPARTMENT,**

**ASSOCIATE PROFESSOR,**

Department of

Department of

Computer science & Engineering ,

Computer science & Engineering ,

PSNA College of Engg.&Tech.,

PSNA College of Engg.&Tech,

Dindigul- 624622

Dindigul- 624622

**Submitted for viva voce examination held on ……………….2018**

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

**ACKNOWLEDGEMENT**

With warm hearts, I feel very pleased to thank the Almighty for his Showers of Grace and Blessings which led me to the successful completion of this project. I would like to express my gratitude towards my parents for their kind co-operation and encouragement which help me in the completion of this project.

We take this opportunity to express my sincere thanks to the respected chairperson **Tmt. K. DHANALAKSHMI AMMAL,** who is the guiding light for all the activities in my college. I would like to express my gratitude to our Pro-Chairman **Rtn**.**Thiru R.S.K Raguraam, D.A.E, M.com, and** Vice-Chairman **Thiru R.S.K Sukumaran, B.A.** for their continuous support towards the student’sdevelopment.

We would like to thank our Principal **Dr.N.Mahendran, M.E., Ph.D**., for being a light in guiding every one of us and infusing us the strength and enthusiasm to work over successfully.

We express all my thanks and gratitude to **Dr.D.SHANTHI, M.E., Ph.D.,** Professor and Head, Department of Computer Science and Engineering for her valuable suggestions and encouragement in the completion of this project work.

The project would not be possible without the motivation and guidance **Dr.S.SATHEES BABU., M.E., Ph.D*.,*** Professor and our Project Guide **Mr.R.KARTHIKEYAN., M.Tech.,** Associate Professor of Department ofComputer Science and Engineering.

**ABSTRACT**

Cloud providers provides various services to customer over a network. This service model offers improved resource flexibility where tenants rent computing resources to operate complex systems. Many organizations operating on sensitive data avoid migrating operations to infrastructure cloud platforms due to security concerns. This project describes a framework for data and operation security in IAAS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. Thus once the user is authenticated they will be launched in virtual machines where they initiate the upload process into the cloud. Also in this proposed system encryption keys are maintained outside of the IAAS domain. RSA algorithm is used for public key encryption. In this proposed system, implementing virtual machines and key management secure data access has been provided.

iv

**TABLE OF CONTENTS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CHAPTER NO** | **TITLE** | | | **PAGE NO** |
|  | **ABSTRACT** | | | iv |
|  | **LIST OF TABLES** | | | viii |
|  | **LIST OF FIGURES** | | | Ix |
|  | **LIST OF ABBREVIATIONS** | | | x |
| **1** | **INTRODUCTION** | | | 1 |
|  | 1.1 PROJECT OVERVIEW | | | 1 |
|  | 1.2 AIM | | | 3 |
|  | 1.3 OBJECTIVE | | | 3 |
| **2** | **SYSTEM ANALYSIS** | | | 4 |
|  | 2.1 EXISTING SYSTEM | | | 4 |
|  |  | 2.1.1 Drawbacks Of Existing System | | 4 |
|  | 2.2 NEED FOR PROPOSED SYSTEM | | | 5 |
|  | 2.3 PROPOSED SYSTEM | | | 5 |
|  |  | 2.3.1 Feasibility Study | | 6 |
|  | 2.4 REQUIREMENT ANALYSIS | | | 7 |
|  |  | 2.4.1 Hardware Requirements | | 7 |
|  |  | 2.4.2 Software Requirements | | 7 |
|  |  |  | 2.4.2.1 Tools | 8 |
|  |  |  | 2.4.2.2 Programming language | 9 |
|  |  |  | 2.4.2.3 Database | 11 |
|  | v  2.5 ASSUMPTIONS AND DEPENDENCIES | | | 11 |
| **3** | **SYSTEM DESIGN** | | | 12 |
|  | 3.1 UML Diagrams | | | 12 |
|  |  | 3.1.1 Use Case Diagram | | 12 |
|  |  | 3.1.2 Class Diagram | | 13 |
|  |  | 3.1.3 Sequence Diagram | | 14 |
|  |  | 3.1.4 Activity Diagram | | 15 |
|  |  | 3.1.5 ER Diagram | | 16 |
|  |  | 3.1.6 System Architecture Diagram | | 18 |
|  | 3.2 DATABASE DESIGN | | | 19 |
|  |  | 3.2.1 Registration Table | | 19 |
|  |  | 3.2.2 File Table | | 20 |
| **4** | **IMPLEMENTATION AND TESTING** | | | 22 |
|  | 4.1 MODULE DESCRIPTION | | | 22 |
|  | 4.1.1 Identity Management | | | 22 |
|  | 4.1.2 Key Generation and Maintenance Scheme | | | 23 |
|  | 4.1.3 Virtual Machine | | | 25 |
|  | 4.1.4 Cloud storage | | | 26 |
|  | 4.1.5 Encryption Algorithm | | | 27 |
|  | 4.2 TESTING | | | 32 |
|  |  | 4.2.1 Unit Testing | | 32 |
|  |  | vi  4.2.2 Integration Testing | | 32 |
|  |  | 4.2.3 Validation Testing | | 32 |
|  |  | 4.2.4 Functional Testing | | 33 |
|  |  | 4.2.5 Structural Testing | | 33 |
|  | 4.3 DRIVING TEST CASES | | | 33 |
| **5** | **CONCLUSION AND FUTURE WORKS** | | | 35 |
|  | 5.1 CONCLUSION | | | 35 |
|  | 5.2 FUTURE WORKS | | | 35 |
|  | **REFERENCES** | | | 37 |

vii

**LIST OF TABLES**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **TABLE NO** | **TABLE NAME** | **PAGE NO** |
| 1 | 3.1 | Registration Table | 20 |
| 2 | 3.2 | File Table | 21 |
| 3 | 4.1 | Test Case Table | 34 |

viii

**LIST OF FIGURES**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **FIGURE NO** | **FIGURE NAME** | **PAGE NO** |
| 1 | 3.1 | Use Case Diagram | 11 |
| 2 | 3.2 | Class Diagram | 14 |
| 3 | 3.3 | Sequence Diagram | 15 |
| 4 | 3.4 | Activity Diagram | 16 |
| 5 | 3.5 | ER Diagram | 17 |
| 6 | 3.6 | System Architecture Diagram | 19 |
| 7 | 4.1 | Generation of security question | 22 |
| 8 | 4.2 | Security question page | 23 |
| 9 | 4.3 | User file list | 24 |
| 10 | 4.4 | User download page | 24 |
| 11 | 4.5 | public key and private key in VM | 25 |
| 12 | 4.6 | public key visible to the user | 26 |
| 13 | 4.7 | Cloudme webpage | 27 |
| 14 | 4.8 | Encryption Algorithm | 30 |
| 15 | 4.9 | Decryption Algorithm | 31 |

ix

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **S.NO** | **ACRONYMS** | **ABBREVIATIONS** |
| 1 | **HTML** | **H**ypertext **M**ark-up **L**anguage |
| 2 | **CSS** | **C**ascade **S**tyle **S**heet |
| 3 | **JS** | **J**ava**S**cript |
| 4 | **XML** | e**X**tensible **M**ark-up **L**anguage |
| 5 | **DB** | **D**atabase |
| 6 | **UML** | **U**nified **M**odelling **L**anguage |
| 7 | **SQL** | **S**tructure **Q**uerying **L**anguage |
| 8 | **JSP** | **J**ava **S**ever **P**age |
| 9 | **IDE** | **I**ntegrated **D**evelopment **E**nvironment |
| 10 | **IAAS** | **I**nfrastructure **A**s **A S**ervice |

x