**PUBLIC VERIFIABILITY FOR ENHANCEMENT OF SECRET DATA DELETION WITH TIMEOUT**

A PROJECT REPORT

*Submitted by*

**Sittukala S (111712104094)**

**Suwetha S (111712104104)**

**Vasavi E (111712104317)**

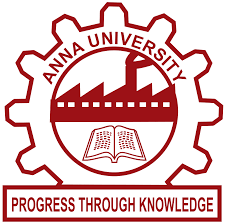
*In partial fulfilment for the award of the degree*

*Of*

BACHELOR OF ENGINEERING

IN

**COMPUTER SCIENCE AND ENGINEERING**

RMK ENGINEERING COLLEGE, KAVARAIPETTAI

ANNA UNIVERSITY: CHENNAI 600 025

APRIL 2016

**ANNA UNIVERSITY : CHENNAI 600 025**

**BONAFIDE CERTIFICATE**

Certified that this project report **“PUBLIC VERIFIABILITY FOR ENHANCEMENT OF SECRET DATA DELETION WITH TIMEOUT”** is the bonafide work of “**Sittukala.S (111712104094)** **Suwetha.S (111712104104), and Vasavi.E (111712104317)”** who carried out the project work under my supervision.

|  |  |
| --- | --- |
| **SIGNATURE**  **DR. K.L.SHANMUGANATHAN, M.E.,M.S.,Ph.D.,** HEAD OF THE DEPARTMENT  PROFESSOR  Department of Computer Science and  Engineering,  R.M.K Engineering College,  Kavaraipettai - 601 206. | **SIGNATURE**  **Mrs.S.RADHIKA, M.E., (Ph. D)**  SUPERVISOR  ASSISTANT PROFESSOR  Department of Computer Science and Engineering,  R.M.K Engineering College,  Kavaraipettai - 601 206. |

Submitted for the Project viva-voice held on -------------------------

External Examiner Internal Examiner

**ABSTRACT**

Existing software-based data erasure programs can be summarized as following the same one-bit-return protocol: the deletion program performs data erasure and returns either success or failure. Here we present a cryptographic solution that aims to make the data deletion process more transparent and verifiable. In contrast to the conventional black/white assumptions about TPM (i.e., either completely trust or distrust), we introduce a third assumption that sits in between: namely, “trust-but-verify”. Our solution enables a user to verify the correct implementation of two important operations inside a TPM without accessing its source code: i.e., the correct encryption of data and the faithful deletion of the key. Finally, we present a proof-of-concept implementation of the SSE system on a resource-constrained Java card to demonstrate its practical feasibility. To our knowledge, this is the first systematic solution to the secure data deletion problem based on a “trust-but-verify” paradigm, together with a concrete prototype implementation.

**ACKNOWLEDGEMENT**

We convey our thanks to our Chairman **Thiru.R.S.Munirathnam** and Vice-chairman **Mr.R.M.Kishore** who took keen interest on us and encouraged throughout the course of study and for their attention and valuable suggestions offered to us throughout the course of study.

We express our sincere thanks to our principal **Dr. Elwin Chandra Monie** for his whole hearted and kind co-operation.

We are highly thankful to our Head of the Department and our project supervisor **Dr.K.L.Shunmuganathan** for supporting and rendering us with all the facilities for undertaking the project. We are also thankful for his support.

Our sincere thanks to our internal guide **Ms. S. Radhika** extended support and guidance in the successful outcome of this project for her encouraging support and guidance in carrying out the project.

Our heartfelt thanks to our Project Coordinator **Ms. T. Sethukkarasi** for her great support and guidance. We extend our thanks to all the facilities of the Department of Computer Science and Engineering who were behind us throughout the course of study.

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | | **PAGE NO** |
|  | **ABSTRACT** | | **III** |
|  | **LIST OF FIGURES**  **LIST OF TABLES** | | **VII**  **VIII** |
|  | **LIST OF ABBREVIATIONS** | | **IX** |
|  |  | |  |
| **1.** | **INTRODUCTION** | | **1** |
|  | 1.1 CLOUD COMPUTING | | 1 |
|  | 1.2 OBJECTIVE | | 3 |
| **2.**  **3.** | 1.3 SCOPE  **LITERATURE SURVEY**  **SYSTEM ANALYSIS**  3.1 OVERALL DESCRIPTION  3.1.1 PROBLEM STATEMENT  3.1.2 EXISTING SYSTEM  3.1.3 PROPOSED SYSTEM  3.2 FEASIBILITY STUDY  3.2.1 ECONONIC FEASIBILITY  3.2.2 TECHNICAL FEASIBILTY  3.2.3 SOCIAL FEASIBILITY | | 3  5  10  10  10  11  12  13  14  14  14 |
| **4.**  **5.** | 3.3 SYSTEM REQUIREMENTS  3.3.1 HARDWARE REQUIREMENTS  3.3.1 SOFTWARE REQUIREMENTS  **SYSTEM DESIGN**  4.1 ARCHITECTURE DIAGRAM  4.2 SYSTEM DESCRIPTION  4.3 DATA FLOW DIAGRAMS  **IMPLEMENTATION DETAILS**  5.1 ALGORITHM  5.2 MODULES  5.3 SECURITY CHECK | | 15  15  15  16  16  17  18  21  21  26  27 |
| **6.**  **7.**  **8.** | **TESTING**  6.1 TYPES OF TESTING  6.2 TEST CASES  **RESULTS AND DISCUSSION**  **CONCLUSION AND FUTURE WORK** | | 30  30  32 |
|  | **APPENDIX 1-SAMPLE CODE**  **APPENDIX 2-SCREENSHOTS** | |  |
|  | **REFERENCES** | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  | **LIST OF FIGURES** |  | |
| **FIGURE NO** | **NAME** | **PAGE NO** | |
| 1.1 | CLOUD DELIVERY MODEL | 2 | |
| 1.2  4.1  4.3.1 | CLOUD DEPLOYMENT MODEL  ARCHITECTURE DIAGRAM  USE CASE DIAGRAM | 3  16  19 | |
| 4.3.2  4.3.3 | CLASS DIAGRAM  SEQUENCE DIAGRAM | 20  21 | |

|  |  |  |
| --- | --- | --- |
|  | **LIST OF TABLES** |  |
| **TABLE NO.** | **TABLE NAME.** | **PAGE NO.** |
| 5.3 | CHALLENGES IN TPM |  |
| 7 | COMPARISON OF SECRET SHARING SCHEME |  |

|  |  |
| --- | --- |
| **LIST OF ABBREVIATIONS** | |
| **ABBREVIATON** | **EXPANSION** |
| JDK  SAAS  PAAS  IAAS  SLA  CSP  TPM | Java Development Kit  Software as a Service  Platform as a Service  Infrastructure as a Service  Service Level Agreement  Cloud Service Provider  Trusted Platform Module |