A PROJECT REPORT

ON

EFFICIENT TRACEABLE AUTHORIZED SEARCH SYSTEM FOR SECURE CLOUD STORAGE

A Project report submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted By

M. Karthik	192P1A0569
M. Mahaboob Basha	192P1A0576
P. Bindu Shruthika	192P1A0596
P. Naga Lakshmi	192P1A0595
M. Mahendra Kumar Reddy	192P1A0575

Under The Esteemed Guidance of

Mr. N. SRINIVASAN M.Tech

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AN ISO 9001:2015 CERTIFIED INSTITUTION

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(Sponsored by Bharathi Educational Society)

(Affiliated to J.N.T.U.A., Anantapuramu, Approved by AICTE, New Delhi)

Recognized by UGC Under the Section 2(f) & 12(B) of UGC Act, 1956

Accredited by NAAC & NBA

Autonomous

Vidyanagar, Proddatur-516360, Y.SR.(Dist.), A.P.

2019 - 2023

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AN ISO 9001:2015 CERTIFIED INSTITUTION

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(Sponsored by Bharathi Educational Society)

(Affiliated to J.N.T.U.A., Anantapuramu, Approved by AICTE, New Delhi)

Recognized by UGC Under the Section 2(f) & 12(B) of UGC Act, 1956

Accredited by NAAC & NBA

Autonomous

Vidyanagar, Proddatur-516360, Y.SR.(Dist.), A.P.

CERTIFICATE

This is to certify that the project work entitled "**EFFICIENT TRACEABLE AUTHORIZED SEARCH SYSTEM FOR SECURE CLOUD STORAGE**" is a bonafide work of M. Karthik (192P1A0569), M. Mahaboob Basha (192P1A0576), P. Bindu Shruthika (192P1A0596), P. Naga Lakshmi (192P1A0595), M. Mahendra Kumar Reddy (192P1A0575) submitted to Chaitanya Bharathi Institute of Technology, Proddatur in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING. The work reported here in does not form part of any other thesis on which a degree has been awarded earlier. This is to further certify that they have worked for a period of one semester for preparing their work under our supervision and guidance.

INTERNAL GUIDE
Mr. N. SRINIVASAN M.Tech
Assistant Professor

HEAD OF THE DEPARTMENT
Mrs. D. Salma Faroze M.Tech
Assistant Professor

PROJECT COORDINATOR
Mr. N. SRINIVASAN M.Tech
Assistant Professor

INTERNAL EXAMINER

EXTERNAL EXAMINER

Certificate

This is to certify that following team members **B.Tech (CSE)** (2019-23) studying final year from **CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY**, Proddatur, YSR Kadapa (dist.), A.P., (Affiliated to J.N.T.U – UNIVERSITY Anantapur, A.P., India), have been successfully completed their **ACADEMIC MAJOR PROJECT** titled "**EFFICIENT TRACEABLE AUTHORIZED SEARCH SYSTEM FOR SECURE CLOUD STORAGE**" by using **JAVA TECHNOLOGY** and other related tools under the guidance of this organization. The following is the list of students who were involved with the design, develop and deployment of the above-mentioned project.

S. No	Roll No	Name	Class
1	192P1A0569	M. Karthik	CSE IV Year
2	192P1A0576	M. Mahaboob Basha	CSE IV Year
3	192P1A0596	P. Bindu Shruthika	CSE IV Year
4	192P1A0595	P. Naga Lakshmi	CSE IV Year
5	192P1A0575	M. Mahendra Kumar Reddy	CSE IV Year

We offered them the complete project guidance & assistance. We place our appreciation on records for their commitment and hard work done during the design & development of this project and the project was completed to our best satisfaction.

Thanks & Regards,

Suman

Trainer

DECLARATION BY THE CANDIDATES

We are M. Karthik, M. Mahaboob Basha, P. Bindhu Shruthika, P. Naga Lakshmi, M. Mahendra Kumar Reddy with respective Roll No : (192P1A0569), (192P1A0576), (192P1A0596), (192P1A0595), (192P1A0575) here by declare that the Project Report entitled "EFFICIENT TRACEABLE AUTHORIZED SEARCH SYSTEM FOR SECURE CLOUD" under the guidance of Mr. N. SRINIVASAN M.Tech, Assistant Professor, Department of CSE is submitted in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science & Engineering.

This is a record of bonafide word carried out by us and the results embodied in the Project Report have not been reproduced or copied from any source. The results embodied in this Project Report have not been submitted to any other University or Institute for the Award of any other Degree or Diploma.

M. Karthik	192P1A0569
M. Mahaboob Basha	192P1A0576
P. Bindu Shruthika	192P1A0596
P. Naga Lakshmi	192P1A0595
M. Mahendra Kumar Reddy	192P1A0575

Dept. of Computer Science & Engineering
Chaitanya Bharathi Institute of Technology
Vidyanagar, Proddatur, Y.S.R.(Dist.)

ACKNOWLEDGEMENT

An endeavour over a long period can be successful only with the advice and support of many well-wishers. We take this opportunity to express our gratitude and appreciation of all of them.

We are extremely thankful to our beloved Chairman **Dr. V. Jayachandra Reddy** who took keen interest and encouraged us in every effort throughout this course.

We owe our gratitude to our Principal **Dr. G. Sreenivasula Reddy** **M.Tech., (PhD).,** for permitting us to use facilities available to accomplish the project successfully.

We express our heartful thanks to **Mrs. D. Salma Faroze** **M.Tech** Head of Dept. CSE for his kind attention and valuable guidance to us throughout this course.

We also express our deep sense of gratitude towards **Mr. N. Srinivasan** **M.Tech**, Dept. CSE for his support and guidance in completing our project.

We express our profound respect and gratitude to our project coordinator **Mr. N. Srinivasan** **M.Tech**, Dept. CSE for his valuable support and guidance in completing the project successfully.

We are highly thankful to **MR. B. SUMAN, MR. G. SANDEEP,** Trylogic Software, Hyderabad, who have been kind enough to guide us in the preparation and execution of this project.

We also thank all the teaching & non-teaching staff of Dept. of CSE for their support throughout our B.Tech course.

We express our heartful thanks to our parents for their valuable support and encouragement in completion of our course. Also, we express our heartful regards to our friends for being supportive in completion of the project.

CONTENT

Table of Contents	Page No
Abstract	**I**
List of Figures	**II**
List of Screens	**III**
1. Introduction	**1 – 5**
1.1 Literature Review	3 - 5
2. System Analysis	**6 – 8**
2.1 Existing System	6 – 7
2.2 Proposed System	7 – 8
3. Requirement Specifications	**9**
4. System Design	**10 – 19**
4.1 System Architecture	10 – 11
4.2 Block Diagrams	12
4.3 UML Diagrams	13
4.3.1 Use case Diagram	14 – 17
4.3.2 Class Diagram	18
4.3.3 Sequence Diagram	19
4.3.4 Activity Diagram	20
5. Coding and Implementation	**21 – 50**
6. Testing	**51 – 53**
1. Introduction	51
2. Types of Testing	51
6.1. Unit Testing	51
6.2. Integration testing	52
6.3. Functional Testing	52
6.4 System Testing	53
6.5 White Box Testing	53
6.6 Black Box Testing	53
6.7 Acceptance Testing	53

7. Results	**54 - 65**
8. Conclusion and Enhancement 8.1 Conclusion 8.2 Future Enhancement	**66** 66 66
9. Appendix	**67 – 74**
10. Bibliography	**75 - 77**
11. Biodata	**78**

ABSTRACT

Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit.

Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this project we propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (EF-TAMKS-VOD).

The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices.

In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded.

Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that EF-TAMKS-VOD is provably secure. Efficiency analysis and experimental results show that EF-TAMKS-VOD improves the efficiency and greatly reduces the computation overhead of users' terminals.

List Of Figures

S.NO	FIG NO	FIGURE NMAE	PAGE NO
1	4.1	System Architecture	10
2	4.2	Block Diagram	12
3	4.3.1.a	Use Case Diagram of Data Owner	14
4	4.3.1.b	Use Case Diagram of Data User	15
5	4.3.1.c	Use Case Diagram of Data KGC	16
6	4.3.1.d	Use Case Diagram of Data Cloud	17
7	4.3.2	Class Diagram	18
8	4.3.3	Sequence Diagram	19
9	4.3.4	Activity Diagram	20

List Of Screens

S.NO	FIG NO	FIGURE NMAE	PAGE NO
1	7.1	Owner Registration Page	54
2	7.2	User Registration Page	55
3	7.3	Owner Login Page	56
4	7.4	User Login Page	56
5	7.5	KGC Login Page	57
6	7.6	Cloud Login Page	57
7	7.7	File Upload Page	58
8	7.8	View Files Page	58
9	7.9	Files Search Page	59
10	7.10	File Download Page	59
11	7.11	File Request Page	60
12	7.12	User Activation Page	60
13	7.13	Owner Activation Page	61
14	7.14	View Data Owner Page	61
15	7.15	View Data User Page	62
16	7.16	File Information Page	62
17	7.17	Generating OTP	63
18	7.18	Download Page	63