A Mini Project Report

on

Cipher Text Policy Attribute Based Encryption

by

D. N. V. Kiranmai

(12WH1A1217)

Department of Information Technology

BVRIT HYDERABAD
College of Engineering for Women
(Approved by AICTE, New Delhi, NBA Accredited and Affiliated to JNTUH, Hyderabad)
Bachupally, Hyderabad – 500090

October, 2019

Department of Information technology

BVRIT HYDERABAD
College of Engineering for Women
(Approved by AICTE, New Delhi, NBA Accredited and Affiliated to JNTUH, Hyderabad)
Bachupally, Hyderabad – 500090

CERTIFICATE

This is to certify that the mini project entitled "**Cipher Text Policy Attribute Based Encryption**" done by **Ms. D. N. V. Kiranmai (12WH1A1217),** of **Department of Information Technology** , is a record of work carried out by her during IV Year I semester.

Ms. S. Rama Devi
Associate Professor
Department of IT

Dr. Aruna Rao SL
Professor & HoD
Department of IT

ACKNOWLEDGEMENTS

We would like to express our sincere thanks to **Dr KVN. Sunitha, Principal**, BVRIT HYDERABAD College of Engineering for Women, for providing the working facilities in the college.

Our sincere thanks and gratitude to **Dr. Aruna Rao SL, Professor and HoD**, Department of Information Technology, BVRIT HYDERABAD College of Engineering for Women for all the timely support and valuable suggestions during the period of our project.

We are extremely thankful and indebted to our internal guide, **Ms. S. Rama Devi, Associate Professor,** Department of Information Technology, BVRIT HYDERABAD College of Engineering for Women for her constant guidance, encouragement and moral support throughout the project.

Finally, we would also like to thank all the faculty and staff of Information Technology Department who helped us directly or indirectly, parents and friends for their cooperation in completing the project work.

D. N. V. Kiranmai
(12WH1A1217)

CONTENTS

ABSTRACT

In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving.

Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in the project.

In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. The project achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.