RESISTING SINGLE POINT OF FAILURE IN CP-ABE WITH SECURE SETUP

By

KHER JAYVIRSINH RAJENDRASINH
Enrollment No.:140370702540

Mr. NARENDRA SINGH
M.Tech (CSE)
Assistant Professor, CSE Department

A **Thesis** Submitted to
Gujarat Technological University in Partial
Fulfillment of the Requirements for
The Degree of Master of Engineering
In **Computer Engineering**

May – 2016

Computer Science & Engineering Department,
Parul Institute of Engineering & Technology
P.O: Limda, Ta.: Waghodia, Dist.: Vadodara

Resisting Single point of failure in CP-ABE with Secure Setup

Submitted By

Jayvir R. Kher

Supervised By

Mr. Narendra Singh

Assistant professor

Parul Institute of Engineering and

Technology, Limda, Waghodia,

Vadodara

ABSTRACT

Attribute Based Encryption was first introduced by Amit Sahai and Brent Waters. It was proposed to solve complex access control mechanism over encrypted data. In Attribute Based encryption the key and ciphertext deal with the set of attributes. There are various schemes available of attribute based encryption e.g. ciphertext-policy attribute based encryption, key-policy attribute based encryption and multiple authority attribute based encryption. In this work we propose resisting single point of failure in ciphertext-policy attribute based encryption with secure setup. Our scheme consists of six algorithms of setup, AA setup, Key Generation, Request Attribute SK, Encryption and Decryption. The features of our schemes is resisting the single point of failure, secure against collusion attack and Scheme is fully secure.