SECURITY OF CONSTANT CIPHER TEXTPOLICY-ATTRIBUTE BASED ENCRYPTION USING PATTERN BASED ALGORITHM

B. VEERAMALLU
(*Professor, Department of Computer Science & Engineering*)
Teegala Krishna Reddy College of Engineering & Technology,
Hyderabad, Telangana, INDIA

CH. V. PHANI KRISHNA
(*Professor, Department of Information Technology*)
Teegala Krishna Reddy Engineering College,
Hyderabad, Telangana, INDIA

SECURITY OF CONSTANT CIPHER TEXTPOLICY-ATTRIBUTE BASED ENCRYPTION USING PATTERN BASED ALGORITHM

ISBN-13: 978-93-87610-41-5
FIRST EDITION, AUGUST 2019, INDIA

Printed & Published by:
VSRD Academic Publishing
A Division of Visual Soft India Private Limited

Printed & Bound in India

VSRD ACADEMIC PUBLISHING
A Division of Visual Soft (India) Pvt. Ltd.

REGISTERED OFFICE
154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)
Mob.: +91 9899936803 ||Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

MARKETING OFFICE
340, First Floor, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI – 400 053 (MH) (INDIA)
Mob.: +91 9956127040 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

PREFACE

Attribute based encryption can be treated as a log encryption where it allows each user to have a unique key, which is defined by their properties. We use Attribute Based Encryption Scheme with Non Monotonic Access Structures which utilize the unconstructive word to depict each property in the information. In this thesis we propose Cipher text – policy attribute based encryption and broad cast encryption scheme.

Cipher text – policy attribute based encryption and broad cast encryption scheme are constructed of constant size CP-ABE for an AND gate access policy, that significantly reduces the cipher text to constant size with any given number of attributes. Each cipher text in CCP-ABE requires 2 elements on a bilinear group. And ABBE is more flexible because a broad casted message can be encrypted by an expressive access policy, either with or without explicit specifying the receivers. More over ABBE significantly reduce the storage and communication over head to the order of O (log N) when N is the system size.

However the security of CCP-ABE is based on selective-ID attackers which are limited to specific attacks only. We propose constructing a new constant CP-ABE pattern based algorithm, which significantly secure against pattern of attackers. Also solving storage over head of ABBE and extending storage with optimization.

Key words: constant-size cipher text-attribute based encryption (CCP-ABE), Attribute Based Broadcast Encryption (ABBE).

✍ *Author(s)*

CONTENTS