

**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 TEXT POLICY-ATTRIBUTE BASED ENCRYPTION USING PATTERN BASED ALGORITHM

Copyright © : Ch V. Phani Krishna
Publishing Right (P) : VSRD Academic Publishing
A Division of Visual Soft India Private Limited

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

Disclaimer: The author(s) are solely responsible for the contents compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Authors or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

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

CHAPTER 1 NETWORK SECURITY – SOME PRELIMINARIES	1
1.1. INTRODUCTION	1
1.2. SECURITY ATTACKS.....	1
1.3. SECURITY REQUIREMENTS.....	4
1.4. HISTORY	4
1.5. LITERATURE SURVEY.....	8
1.6. HOW IT WORKS	12
1.7. EXISTING SYSTEM	16
1.8. ADVANTAGES	18
1.9. DISADVANTAGES.....	18
1.10. PROPOSED WORK.....	18
1.11. CONCLUSION	21
1.12. RELEVANT LITERATURE SURVEY FOR THE PROPOSED STUDY.....	21
CHAPTER 2 : CONSTANT CIPHER TEXT APPROACH ATTRIBUTE BASED ENCRYPTION	24
2.1. INTRODUCTION	24
2.2. RELATED WORK	25
2.3. PATTERN BASED ENCRYPTION ALGORITHM.....	27
2.4. EXPERIMENTAL RESULTS	29
2.5. CONCLUSION	33
CHAPTER 3 : TO DIPPING THE OVERHEADS OF CCP-ABE, USING PATTERN BASED POLICY WITH HOMOMORPHISM ENCRYPTION MECHANISM	34
3.1. INTRODUCTION	34
3.2. RELATED WORK.....	36
3.3. REDUCTION OF STORAGE OVERHEAD AND TIME COMPLEXITY USING PROPOSED PATTERN BASED ENCRYPTION ALGORITHM.....	37
3.4. EXPERIMENTAL RESULTS	46
3.5. CONCLUSION	48
CHAPTER 4 : MINIMIZING COMPUTATION AND COMMUNICATION OVERHEAD UTILIZATION PATTERN BASED HOMOMORPHISM ENCRYPTION	49
4.1. INTRODUCTION	49
4.2. RELATED WORK	50
4.3. REDUCING COMPUTATION AND COMMUNICATION OVERHEAD	52

4.4.	EXPERIMENTAL RESULTS	53
4.5.	CONCLUSION	56
CHAPTER 5 : SUMMARY AND CONCLUSION		57
CHAPTER 6 : REFERENCES.....		58