A Survey Of Attribute-based Encryption Schemes

Qxx

***Abstract*—The abstract goes here.**

***Index Terms*—The keywords goes here[1].**

I. Introduction

Attribute-based encryption(ABE) play an important role in encryption scheme of cloud such us[**?**],[**?**],[**?**],[**?**],[**?**] due to that ABE is not only powerful mechanism for protecting the confidentiality of stored and transmitted information inheriting traditional public-key encryption but also achieves the stride from one-to-one model from previous encryption to one-to-many[**?**],and specifically implementing access control and supporting storing in untrusted storage server are the reasons for its achieving.Additionally,ABE has following concrete advantages:

1) High Efficiency: :The cost of encryption and decryption is only related with the length of ciphertext and the number of attributes,and has nothing to do with the number of users;

2) Dynamic: :decryption can be completed by user only when the attributes satisfy the policy,and has nothing to do with the time when the user join this systems.

3) Flexibility: :ABE supports various access structure such us threshold policy and boolean format.

4) Privacy: :when data owner encrypt,he or she has no need to know the specific identities of individuals who will authorised decrypt[**?**].

ABE is actually an extension of identified based encryption(IBE) and it can regard as a special IBE that multiply identities which meet a specific constraint can decrypt the ciphertext.In ABE,that constraint is just the access policy,and user can decrypt only when attributes satisfy the policy.For integrity,there is a simple division,which is only helpful on the application context and make little sense for the more heuristic research on ABE after it has formed,of ABE into ciphertext-policy attribute-Based encryption(CP-ABE) and key-policy attribute-Based encryption(KP-ABE).For CP-ABE,user keys are associated with sets of attributes,whereas ciphertexts are associated with policies,and for KP-ABE,the case is the contrary.

With the development of heuristic research on ABE,more and more ABE variants has been growing.However,there has been no integrated overview published that should not just concludes most of topics of ABE but also figure out the logical and clear clues or veins of development of ABE from pre-birth to now.[**?**]does the survey on ABE of access control,but just enumerate CP-ABE,KP-ABE,ABE Scheme with Non-Monotonic Access Structures,and Hierarchical ABE so from this article we can't find out the relationship among those schemes.From the aspect of difficulties of ABE,[**?**] analyzes the access structure,attribute revocation,key-abuse problem and multi-authority scheme,but those issues don't contain all of that in ABE.[**?**] points out the direction of development on concrete topics of ABE,however there is also no clear hierarchy of ABE schemes.

this is thanks

A. Motivation And Contributions

When everything occurs to us,the ultimate questions of which we would like to know the answer are always about past,now,and future.Now those happen to ABE.Detailedly,the three questions are:

1) Where does ABE come from?:

2) Whats the essence of ABE?and how is it going?:

3) where will ABE go?: Our motivation is finding out the answers of these three questions.

As for our contributions,the first is figuring out the logical and clear clues of the development of ABE based on present ABE schemes,and the clues are helpful to that researchers on ABE can follow specific directions to more exploration and that related others can get clear and integrated general view of ABE.Then we propose a taxonomy which contains all or most ABE schemes,and the taxonomy can be used by researchers to answer many important questions such us:

4) what's the reasons for emergences of those kinds of ABE schemes?:

5) what's the relationship among ABE schemes?:

6) what's the more possible work along developed directions of ABE?: Additionally,this paper explores the design philosophy of classical ABE schemes,which can be a reference for researchers when he or she wants to find the principles of some schemes.After all above,we propose some foresight about the future of ABE.

B. Organization

Organization goes here.

II. clues of the development of ABE

here

A. State-of-the-Art Of ABE

State-of-the-Art of ABE goes here

B. clues of the development of ABE

here

III. Syntax of ABE Schemes

Syntax of ABE Schemes goes here,and don't contain security.

IV. Design Philosophy Of Classical ABE Scheme

some introduction goes here

A. KP-ABE

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent Waters in Proc of Acmccs- 2006

B. CP-ABE

Ciphertext-Policy Attribute-Based Encryption John Bethencourt Amit Sahai Brent Waters in 2007 IEEE Symposium on Security and Privacy 2007

V. Access Control In ABE

some introduction

A. Access Structure

some introduction

1) Monotonictity: Monotonictity goes here

2) Expressive Formula: expressive formula goes here

B. Extension

hierarchy ABE introduction goes here

VI. Research On The Developed Direction Of ABE

some introduction

A. Function

some introduction

1) Proxy Re-encryption: proxy re-encryption ABE goes here

2) Multi-authority: multi-authority ABE and distributed ABE in here

B. Efficiency

some introduction

1) General Technology: outsource and constant ciphertext in ABE goes here

2) Specific Technology: Some examples of Specific Technology in here

C. Security

some introduction

1) Theoretical security: some introduction and security model goes here

2) Applied security: some introduction and collusion problem,abuse key problem,hidden-policy problem,revocation problem go here

VII. Comparison

comparison among some goes here

VIII. Extension

extension goes here. find some interdiscipline topics such as combined with searchable scheme.

IX. Conclusion

The conclusion goes here.

X. Future Of ABE

The future goes here.

References

[1] J. Donald and M. Martonosi, "Techniques for multicore thermal management: Classification and new exploration," in *Proc. Int. Symp. on Computer Architecture (ISCA)*, June 2006, pp. 78–88.

aaa Biography text here.

bbb Biography text here.

ccc Biography text here.