**Hidden Ciphertext Policy Attribute-BasedEncryption Under Standard Assumptions**

**ABSTRACT:**

We propose two new ciphertext policy attributebasedencryption (CP-ABE) schemes where the access policyis defined by AND-gate with wildcard. In the first scheme,we present a new technique that uses only one group elementto represent an attribute, while the existing ABE schemes ofthe same type need to use three different group elements torepresent an attribute for the three possible values (namely,positive, negative, and wildcard). Our new technique leads toa new CP-ABE scheme with constant ciphertext size, which,however, cannot hide the access policy used for encryption. Themain contribution of this paper is to propose a new CP-ABEscheme with the property of hidden access policy by extendingthe technique we used in the construction of our first scheme.In particular, we show a way to bridge ABE based on AND-gatewith wildcard with inner product encryption and then use thelatter to achieve the goal of hidden access policy. We prove thatour second scheme is secure under the standard decisional linearand decisional bilinear Diffie–Hellman assumptions.

**EXISTING SYSTEM:**

* In a CP-ABE, the user’s attributes used for key generation must satisfy the access policy used for encryption in order to decrypt the ciphertext, while in a KP-ABE, the user can only decrypt ciphertexts whose attributes satisfy the policy embedded in the key. We can see that access control is an inherent feature of ABE, and by using some expressive access structures, we can effectively achieve fine-grained access control.
* The fuzzy IBE given by Sahai and Waters, whichcan be treated as the first KP-ABE, used a specific thresholdaccess policy.
* Later, the Linear Secret Sharing Scheme (LSSS)realizable (or monotone) access structure has been adopted bymany subsequent ABE schemes.
* Cheung and Newport proposed another way to define accessstructure using AND-Gate with wildcard.Cheung and Newport showed that by using this simple accessstructure, which is sufficient for many applications, CP-ABEschemes can be constructed based on standard complexityassumptions.
* Subsequently, several ABE schemeswere proposed following this specific accessstructure.

**DISADVANTAGES OF EXISTING SYSTEM:**

* The existing ABE schemes based on AND-Gate with wildcard cannot achieve this property.
* ABE can well protect the secrecy of the encrypted data against unauthorisedaccess, it does not protect the privacy of the receivers/decryptors by default.That is, given the ciphertext, an unauthorised user may still be able to obtain some information of the data recipients.
* Although a secure ABE can well protect the secrecy of theencrypted data against unauthorised access, it does not protectthe privacy of the receivers/decryptors by default. That is,given the ciphertext, an unauthorised user may still be able toobtain some information of the data recipients. For example,a health organization wants to send a message to all the patients that carry certain diseases. Then the attribute universewill contain all the diseases, and an access policy will have theformat “++−∗∗+*. . .*” where “+” (“−”) indicates positive(negative) for a particular disease.
* If a CP-ABE cannot hide theaccess policy, then from the fact whether a person can decryptthe message or not, people can directly learn some sensitiveinformation of the user. Therefore, it is also very importantto hide the access policy in such applications. However,most of the existing ABE schemes based on AND-Gate withwildcard cannot achieve this property.

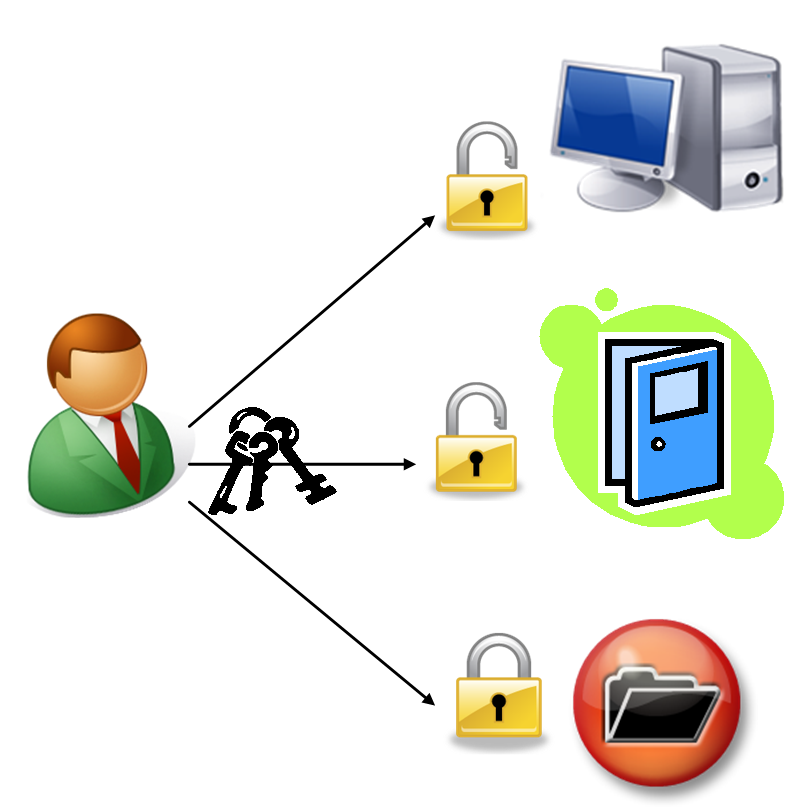
**PROPOSED SYSTEM:**

* In this work, we explore new techniques for the constructionof CP-ABE schemes based on the AND-gate with wildcardaccess structure. The existing schemes of this type need touse three different elements to represent the three possiblevalues – positive, negative, and wildcard – of an attribute in theaccess structure.
* In this paper, we propose a new constructionwhich uses only one element to represent one attribute. Themain idea behind our construction is to use the “positions”of different symbols to perform the matching between theaccess policy and user attributes.
* Specifically, we put theindices of all the positive, negative and wildcard attributesdefined in an access structure into three sets, and by using thetechnique of Viète’s formulas, we allow the decryptor toremove all the wildcard positions, and perform the decryptioncorrectly if and only if the remaining user attributes matchthose defined in the access structure.
* We further study the problem of hiding the access policy forCP-ABE based on AND-Gate with wildcard. As the main contributionof this work, we extend the technique we have used inthe first construction to bridge ABE based on AND-Gate withwildcard with Inner Product Encryption (IPE).
* Specifically, we present a way to convert an access policycontaining positive, negative, and wildcard symbols into avector \_*X* which is used for encryption, and the user’s attributescontaining positive and negative symbols into another vector \_ *Y*which is used in key generation, and then apply the techniqueof IPE to do the encryption.

**ADVANTAGES OF PROPOSED SYSTEM:**

* Our new technique leads to a new CP-ABE scheme with constant ciphertext size.
* The system have used in the first construction to bridge ABE based on AND-Gate with wildcard with Inner Product Encryption (IPE).
* Our first schemeachieves constant ciphertext size.
* Secure under the DecisionalBilinear Diffie-Hellman and the Decision Linear assumptions.

**SYSTEM ARCHITECTURE:**



**MODULES:**

* Owner
* User
* Admin

**MODULES DESCRIPTION:**

Owner:

* Owner Will Sign up and Wait for the authorization (key) of admin.
* After Getting key Owner can login using the key,and upload any personal file by encrypting using ABE with wildcard characters on the cloud.
* Owner will check the progress status of the file upload by him/her.
* Owner logout the session.

**User:**

* User will register and wait for the authorization(key) of admin.
* User will login and access file using the same attribute for decrypt
* User view the file and download the file
* User logout the session.

**Admin:**

* Admin Will Login on the admin's page.
* He/she will check the pending requests of any of the above person.
* Admin check the download/session history user for future referral
* Admin logout session

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

Tran Viet Xuan Phuong, Guomin Yang, *Member, IEEE*, and Willy Susilo, *Senior Member, IEEE,* “Hidden Ciphertext Policy Attribute-BasedEncryption Under Standard Assumptions”, **IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 1, JANUARY 2016.**