Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 06, Issue, 05, pp. 7853-7857, May, 2016

Full Length Research Article

INSPECTING CLOUD STORAGE VIA DENIABLE ATTRIBUTE BASED ENCRYPTION

***Chitra Devi, D. and Sivakani, R.**

Department of Computer Science, Apollo Engineering College, India

ARTICLE INFO

Article History:

Received 25th February, 2016
Received in revised form
18th March, 2016
Accepted 17th April, 2016
Published online 31st May, 2016

Key Words:

Cloud,
Encryption,
Cloud Storage.

ABSTRACT

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with afine-grainedac- cesscontrol mechanism. Our proposed scheme provides a possible waytofightagainst immoralinterference with the right of privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant.In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies.Once cloud storage providers are compromised, all encryption schemes lose their effectiveness.

****Corresponding author: Chitra Devi, D.,***
Department of Computer Science, Apollo Engineering College, India

Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lavabit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service.Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called deniable encryption. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme.

Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have systemwide secrets and must be able to decrypt all encrypted data1. In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme.We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

Related Works

In (Sahai and Waters, 2005), Fuzzy identity based Encryption was proposed, which introduces a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper it presents two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. It proves the security of our schemes under the Selective-ID security model.

In (Goyal *et al*., 2006), Attribute-based Encrption for fine-grained access control of encrypted data was introduced, in which more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

In (Bethencourt *et al*., 2007), Ciphertext policy attribute based Encryption was proposed, In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous AttributeBased Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

Proposed System

The proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. We proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism.

System Architecture

A system architecture as shown in Fig.1. is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organised in a way that supports reasoning about the structures and behaviours of the system.

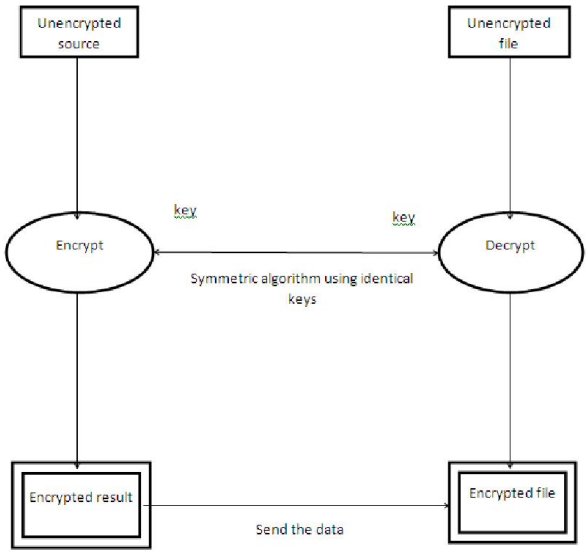


Fig.1. System Architecture

Class Diagram

A class diagram as shown in Fig.2. is an illustration of the relationshis and source code dependencies among claases in the UML.In this context, a class defines the methods and variables in an object,which is a specific entity in a program or the unit of code represening the entity.

Collaboration Diagram

Like sequence diagrams, collaboration diagram as shown in Fig.3. are also interaction diagrams. Collaboration diagrams convey the same information as sequence diagrams, but focus on object roles instead of the times that messages are sent.

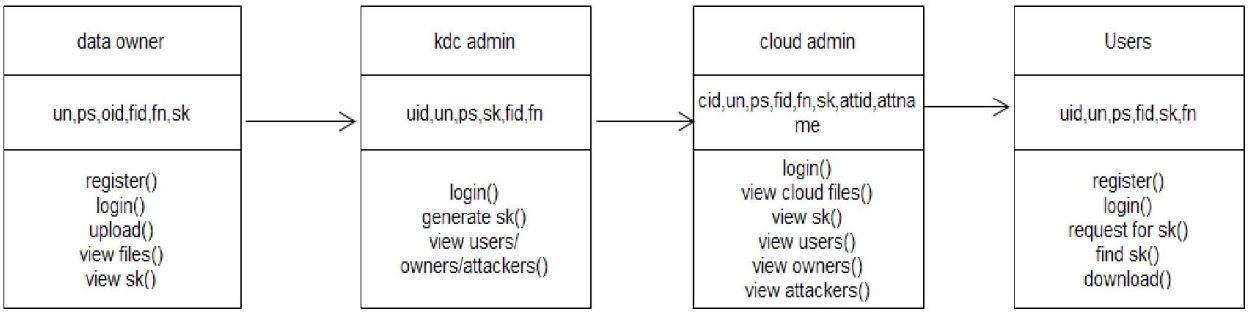


Fig. 2. Class Diagram

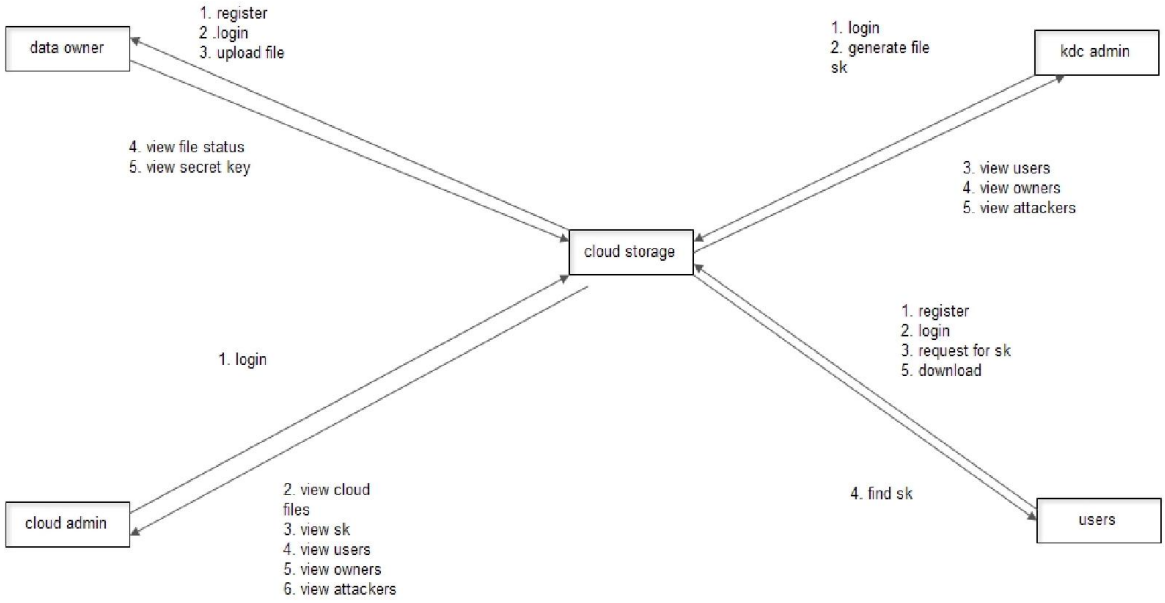
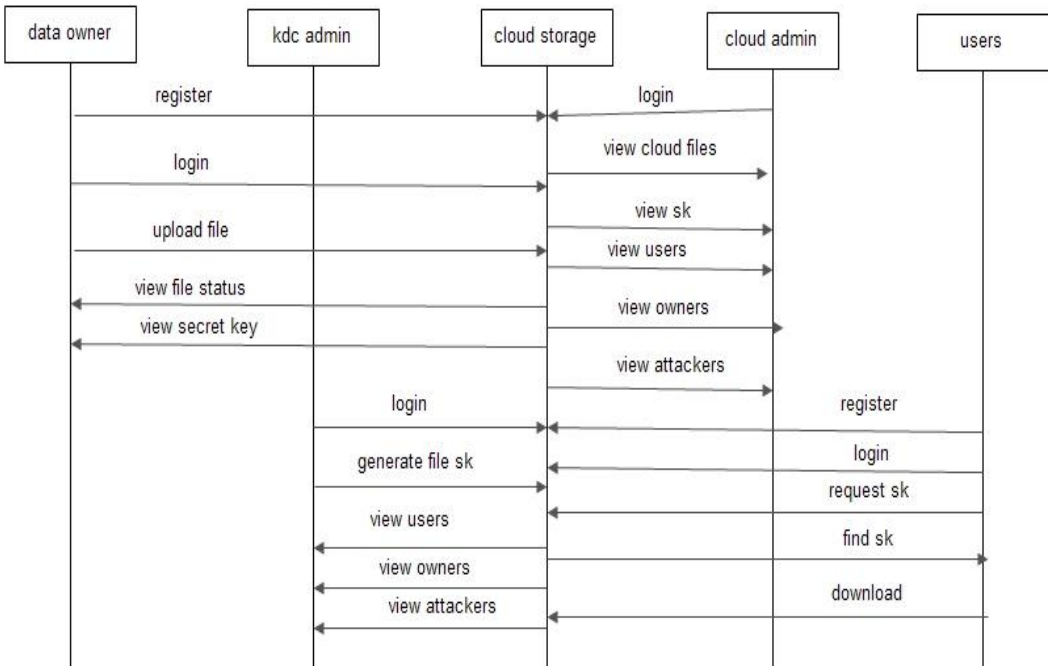


Fig. 3. Collaboration Diagram



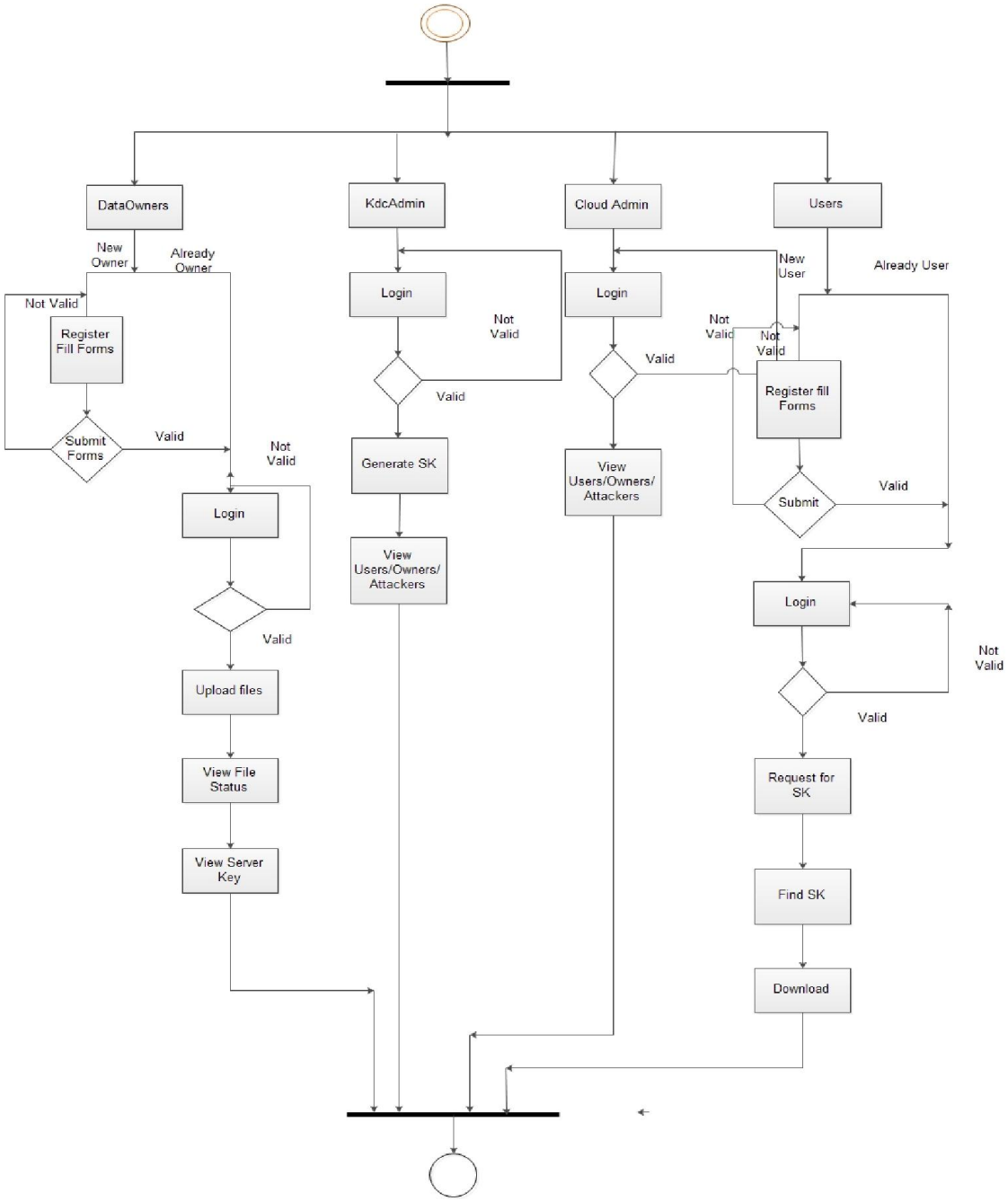


Fig. 5. Activity Diagram

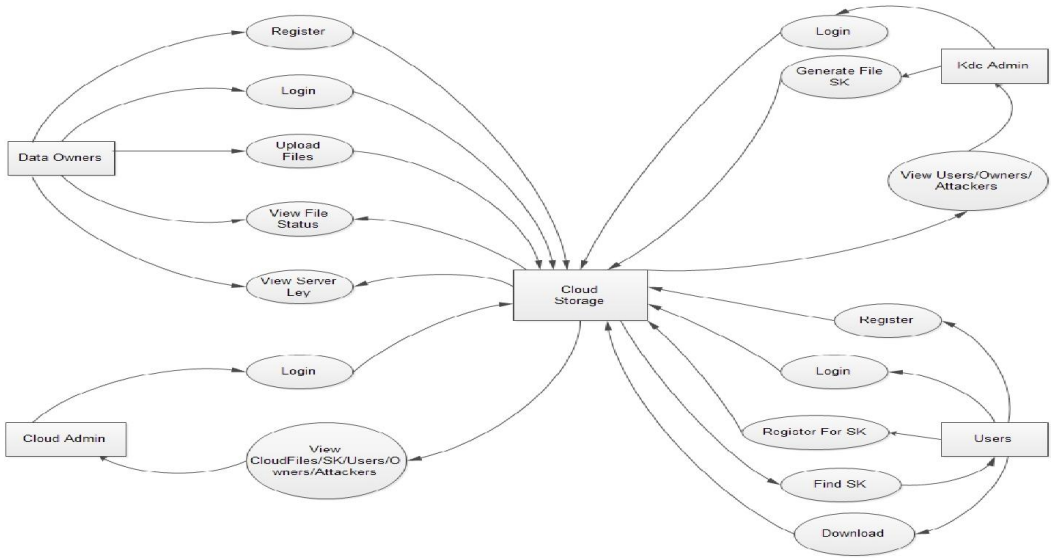


Fig. 6. Data Flow Diagram

Sequence Diagram

A sequence diagram as shown in Fig.4. is an interaction diagram that details how operations are carried out;what messages are sent and when sequence diagrams are organiswed according to time.The time progresses as you go down the page.

Activity Diagram

Activity diagram as shown Fig.5. are graphical representations of workflows of stepwise activities and actions with support for choice,iteration and concurrency.In the UML,activity diagrams are intended to model both computational and organisational processes(i.e.workflows).

Data Flow Diagram

The *Data Flow Diagram* (DFD) as shown in Fig.6. is a graphical representation of the flow of data through an information system. It enables you to represent the processes in your information system from the viewpoint of data. The DFD lets you visualize how the system operates, what the system accomplishes and how it will be implemented, when it is refined with further specification.

Conclusion and Future Enhancements

In this work, we proposed a deniable CP-ABE scheme tobuild an audit-free cloud storage service. The deniabilityfeature makes coercion invalid, and the ABE propertyensures secure cloud data sharing with a fine-grained accesscontrol mechanism. Our proposed scheme providesa possible way to fight against immoral interference withthe right of privacy. We hope more schemes can becreated to protect cloud user privacy. Furthermore, we provide this authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure, and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud storage system.

REFERENCES

Attrapadung, N. Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., and Ràfols, C., "Attribute-based encryption schemes with constant-sizecipher texts," *Theor. Comput. Sci.*, vol.422, pp. 15–38, 2012.

Bethencourt, J., Sahai, A., and Waters, B. 2007. "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334.

Canetti, R. Dwork, C., Naor, M. and Ostrovsky, R. 1997. "Deniable encryption," in *Crypto*, pp. 90–104.

Dürmuth, M. and Freeman, D. M. 2011. "Deniable encryption with negligible detection probability: An interactiveconstruction,"in *Eurocrypt*, pp. 610–626.

Gasti, P., Ateniese, G., and Blanton, M. 2010. "Deniable cloud storage: sharing files via public-key deniability," in *WPES*, pp. 31–42

Goyal, V., Pandey, O., Sahai, A., and Waters, B. 2006. "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, pp. 89–98.

Hohenbergerand, S. Waters, B. 2013. "Attribute-based encryption with fast decryption," in *Public Key Cryptography*, pp. 162–179.

Klonowski, M., Kubiak, P. and Kutylowski, M. 2008. "Practical deniable encryption," in *SOFSEM*, pp. 599–609.

Lewko, A.B., T., Okamoto, A., Sahai, K., Takashima and B. Waters, 2010. "Fully secure functiona lencryption: Attribute-based encryption and (hierarchical) inner produc tencryption," in *Eurocrypt*, 2010, pp. 62–91.

O'Neill, A., Peikert, C., and Waters, B. 2011. "Bi-deniable public-key encryption," in *Crypto*, pp. 525–542.

Sahai, A. and Waters, B. 2005. "Fuzzy identity-based encryption" in *Eurocrypt*, pp. 457–473.

Sahai, A., Seyalioglu, H. and Waters, B. 2012. "Dynamic credentials and ciphertext delegation for attribute-basedencryption," in *Crypto*, pp. 199–217.

Tysowski, P.K. and Hasan, M. A. 2013. "Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds." *IEEET. Cloud Computing*, pp. 172–186.

Waters, B. 2011. "Ciphertext-policy attribute-based encryption: An ex- pressive, efficient, and provably secure realization," in *Public Key Cryptography*, pp.53–70.

****