International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

AN ATTRIBUTE BASED APPROACH TO IMPROVE PRIVACY AND SECURITY IN DECENTRALIED CIPHERTEXT – POLICY

Darga Shaik Arshad Roshan
PG Scholar, Department of Information Technology , Shadan College of Engineering and Technology , Hyderabad , Telangana, India - 500086.
Email :- Md.arshadroshan@gmail.com

Subramanian K.M
Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India – 500086. Email: kmsubbu.phd@gmail.com

Md. Ateeq Ur Rahman
Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad, Telangana, India - 500086
Email:- mail_to_ateeq@yahoo.com

***Abstract*— We present an efficient cryptographic solution to implement fine-grained access control on encrypted data in scattered environments using Attribute Based Encryption (ABE). In contrast, the existing privacy preserving multi-authority attribute based encryption (PPMA-ABE) schemes are centralized and have been designed primarily to protect only the GID, thus exposing valuable attributes of the user and allowing for identity inference attacks. To overcome these drawbacks, we propose a privacy-preserving decentralized Ciphertext-Policy Attribute-Based Encryption (PPDCP-ABE) scheme in this study to improve the security and privacy in decentralized access control systems. In the proposed structure, there are multiple authorities that operate without having to rely on an authority to start up the system or generate the secret key. This will help the users to retrieve the secret key corresponding to the attributes without revealing the identity and attribute information of the user. The proposed approach reduces the risk of collusion and dependency on trust between authorities by combining anonymous credential concepts with the use of decentralized key management. Furthermore, it provides the flexibility to have varying access modalities and authorities engagement dynamics without changing the system itself. The proposed solution offers a secure and privacy-preserving decentralised system for sharing and controlled access to encrypted data.**

"Keywords— Attribute-Based Encryption (ABE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Privacy Preservation, Decentralized Access Control, Multi-Authority Encryption, Secure Data Sharing."

I. INTRODUCTION

In the context of the ever increasing presence of distributed computing, cloud storage and networked information systems, there are significant challenges in the secure and controlled access to sensitive data. The traditional public key cryptography is effective if the two parties to the communication are known to each other. However, in most applications, access control needs to be based on attributes of the users and not their identities. To overcome this issue, a flexible cryptographic approach, called ABE, was proposed that allows encryption and decryption to be done by descriptive features rather than by direct user IDs [3]. Further advances have furthered this idea to CP-ABE, where access policies are embedded in the ciphertexts and fine-grained access control is provided over the encrypted content [4]. These developments formed an excellent basis for safe data sharing among decentralized entities [6].

The existing ABE schemes, however, are typically based on a central authority to configure the system, distribute keys and manage attributes. This centralization is limiting on the scalability of the system, and introduces questions about the trust, privacy and robustness of the system. To overcome the single authority problem, multi-authority attribute based encryption scheme is proposed, where each authority has disjoint sets of attributes [10]. Subsequent studies explored privacy-preserving approaches and decentralized architectures to further bolster privacy and reduce the extent of collaboration with law enforcement entities [11]. But user privacy remains challenging as authorities can still derive sensitive information from user linked qualities.

Whereas in real-world use, an individual's characteristics alone have the potential to provide identification data even if there are no direct identifiers present. But combining attributes across multiple authorities and then analysing them introduces the potential for profiling, inferring information not given by the subject and for personal information being leaked. Even though some privacy-preserving decentralized encryption schemes have tried to conceal the identities of the user and enhance the level of privacy in the confidentiality of attribute information, the full protection of both users' identity and sensitive attribute data is still a big issue in the security of access control schemes [12, 13].

To overcome these drawbacks, this paper suggests a secure information sharing system to overcome the reliance on centralized trust model and introduce a decentralized ciphertext-policy framework based on privacy. The proposed work is about the principles of confidentiality in authorisation and facilitates the involvement of independent authorities and

policy-based access control. Secure data access, decentralized deployment environment, and more trusted and scalable encrypted data sharing systems are emphasized in this work by focusing on user identification and attribute information privacy protection.

II. Related Work

With the increasing volume of sensitive data exchanged between various users and domains, security and privacy-aware access control is becoming a crucial requirement in distributed computing and cloud-based information systems. Traditional encryption methods ensure confidentiality but they are not able to provide flexible authorization policies that enable access decisions based on user attributes rather than stated identities. To solve this problem, ABE has been proposed as a cryptographic system for encryption and decryption based on a set of descriptive attributes of individuals and data resources [3]. This paradigm was an important step towards fine-grained access control as it allows data owners to specify criteria under which encrypted information can be accessed.

Subsequent progress has been made to more expressive and policy-driven systems of ABE. With the help of attribute-based fine-grained access control systems, secure data exchange was achieved and reliance on identity-based authorization schemes was decreased [6]. Further advances lead to the development of CP-ABE, in which the access restrictions are directly incorporated into the encrypted material, and users have secret keys associated with attributes [4]. More recent studies [5, 9] enhance the expressiveness of the policy and the guarantees offered by security, potentially allowing for more flexible access architectures and better realizing the encryption under realistic deployment scenarios. These developments have made CP-ABE more useful in certain settings where information requirements are dynamic and regulated, such as in dispersed settings.

Although CP-ABE enhanced the policy-based authorization, most of the previous schemes heavily depended on the central authority to initialize the system, create keys and control attributes. This dependency posed problems with scalability, centralization of trust and single-point-of-failure risks. To resolve these problems, MA-ABE schemes have been proposed to distribute the attribute management across many independent authorities, and reduce the dependency on centralized authorities [10]. The study of threshold and decentralized authority management explored ways to improve resilience of the system and reduce the coordination overhead for the organizations involved [16]. Distributed cryptographic bases have also been useful for ensuring securing authority operations and key management in decentralized systems [17].

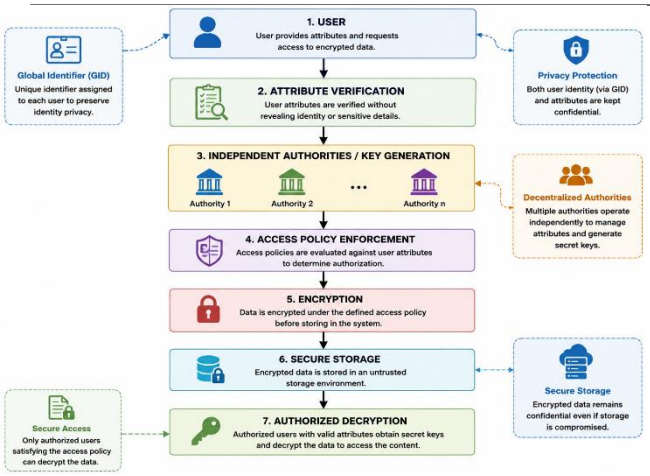
With the evolution of distributed architectures, it became more and more relevant to protect user privacy. In existing multi-authority schemes, users usually need to reveal the IDs and attribute information to the authorities when they are issued with keys, which results in the possibility of attribute aggregation and identity inference. To prevent this exposure, multi-authority encryption systems were suggested [11] which added means to conceal the user identity and improve the confidentiality level of the authorization mechanisms. The idea of anonymous credentials [2] also demonstrated that it was possible for users to prove ownership of attributes without revealing too much identity information, thus offering a more solid base for privacy-preserving access control [2]. In recent papers, these ideas have been extended to decentralized key-policy and ciphertext-policy systems that sought to achieve privacy and to minimize the amount of cooperation among authorities [12, 13].

However, these advances do not address a number of restrictions. Current solutions focus mostly on the protection of user identities with limited protection for sensitive attribute information. Further, partial authority collaboration is still used in some decentralized schemes, or they might fail to prevent privacy leakage by attribute disclosure and inference. Even in the obfuscated case, however, in practice, the user attributes themselves can be used to obtain private identity information. Therefore, a decentralized ciphertext-policy framework is still needed, which, while maintaining the confidentiality of the user identity, would also maintain the confidentiality of the attribute, and would allow the independent participation of authorities without needing to depend on a central point. The above restrictions push forward the proposed approach that tries to enhance the privacy protection and access control in decentralized encrypted environment by employing independent authority management and confidentiality-aware authorization mechanisms [1].

III. Materials And Methods

A) System Overview

The proposed technique proposes a privacy preserving decentralized Ciphertext-Policy Attribute Based Encryption (PPDCP-ABE) scheme which is used for safe data exchange and access management in decentralized contexts. The proposed architecture reduces the reliance on a single trusted authority, as many authorities are able to independently control attributes and distribute keys, compared to the centralized encryption system. These policies enforce access to encrypted data based on attribute, instead of being explicitly based on the identity being revealed. To protect the privacy of users, each user has a GID that binds secret keys in a secure manner, but does not disclose the identity of the user throughout the access request and permission processes. Furthermore, this framework centers on safeguarding delicate attribute data, which limits exposure of such information and improper profiling. The proposed solution aims to offer secure, private and scalable access control for the sharing of encrypted data while decentralizing the participation of authorities and reducing unnecessary revelation of user information in access control settings.



"Fig.1 System Architecture"

The designed architecture of privacy-preserving decentralized CP-ABE system for secure and controlled data access is depicted in Fig.1. The framework begins with verifying attributes and identity of the users. Then independent authority involves in key generation and access management. Access permissions are enforced before the data is encrypted and stored securely with attribute-based policies. The GID can be then used to decode and access the protected material, ensuring GID confidentiality and attribute privacy of authorized users.

B) System Entities and Their Role

The proposed privacy-preserving decentralized CP-ABE scheme requires many entities to cooperate and enable secure and limited access to the encrypted data. Cryptographic keys are issued by independent agencies and there is no central coordination for attribute verification. Data owner uploads protected data to the system and orients the access conditions, which are based on attributes, to the allowed users. Users want to enter the system, and are given permission based on predetermined policies. To improve privacy protection, each user is bound to a GID to make sure that no information identifying a user can be leaked during authorization, even though the users are made unique. The storage environment stores the encrypted files, and ensures that the data itself is kept secure until the requirements for accessing are met. The roles and security responsibilities of each entity are summarised in Table 1.

"Table 1. Roles of System Components"

Entity	Function	Security Responsibility
Authority	Generates and distributes public/private keys and manages attributes	Supports decentralized key management and secure authorization
Data Owner	Uploads encrypted files and defines access conditions	Protects data confidentiality and access policies
User	Requests access and retrieves authorized content	Accesses data only after satisfying authorization requirements
Global Identifier (GID)	Provides unique user association	Preserves identity privacy and prevents identity disclosure
Storage Environment	Stores encrypted files and protected resources	Maintains confidentiality of stored encrypted information

C) Access Control and Privacy Preservation Model

The proposed framework is based on the attribute based paradigm for controlling secure accesses to the encrypted data without compromising the privacy of the users in the decentralized environment. Access choices are enforced with ciphertext-policy schemes where access restrictions are embedded in the encrypted data and those attributes that make up the access policy must be held by the user in order for the access-constrained content to be made available to him. To provide a higher level of privacy, each user is given an identifier, known as a GID, to use for secure authorization without revealing anything about the user during key acquisition process. Plus, critical attribute data is protected to minimize identity inferences and inadvertent profiling. Attribute maintenance and key distribution are separate processes, which decreases dependence on central administration, and unnecessary collaboration between authorities. The system also takes advantage of privacy preserving key delivery mechanisms for secret authorization and to prevent malicious users from accessing the resources that are encrypted.

D) Operational Workflow

The operational workflow of the proposed privacy-preserving decentralized CP-ABE framework depicts the sequence of operations in safe data exchange and controlled access management as shown in Fig. 2. This process begins with the user's onboarding and authorization initiation . Next, is the decentralized key generation, encrypted data storage, and secure data access. Every step helps ensure privacy is preserved, provides attribute-based access policies and reduces reliance on centralized control mechanisms.

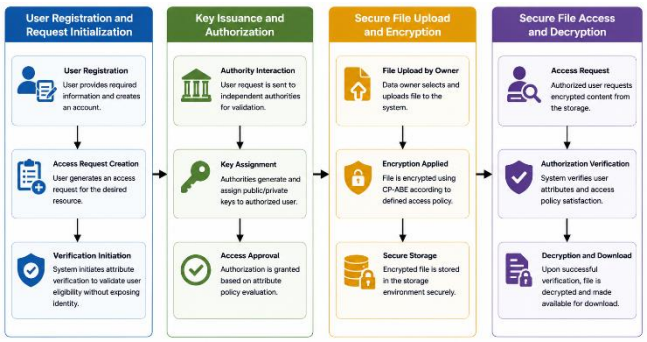
a. User Registration and Request Initialization: The process begins with users' registration, where the users

provide the information to enter the safe access environment. Users send an access request to get the authorization to protected resources when registration is successfully completed. At this stage, the level also starts to verify attributes to determine if the user is eligible without revealing any sensitive identifying information. The registration and request initialization processes lay the groundwork for safe communications between users and involved authorities, and safeguarding of privacy requirements.

b. Key Issuance and Authorization: The decentralized authority mechanism performs the permission and key issuing actions after the generation of the requests. Independent authorities help in validating user requests and in controlling access privileges based on attribute requirements. Authorized parties are given and produce public and private keys to encrypt data and ensure secure communications. Then authorization decisions are based on the pre-defined access policy to allow only legitimate users to get valid authentication data to continue the process.

c. Secure File Upload and Encryption: The data owner uploads files into the secure environment to be stored safely and distributed according to regulations after authorization. Access is controlled and files uploaded are encrypted prior to storage to ensure confidentiality. The encrypted files are then transferred to the storage system that offers protection against illegal access and direct exposure to the files.

d. Secure File Access and Decryption: At the last stage, the authorized users seek access to the encrypted resources in the storage environment. The system verifies that the user is authorized and access conditions are met prior to retrieval. If the validation is successful, the encrypted content will be decrypted using supplied credentials and downloadable. With this method, only users with the correct authorization will be able to view secure data.



"Fig.2 Operational Workflow of Proposed Framework"

E) Implementation Environment

The prototype of the file sharing application that was researched was built in such a way that it would be a secure file sharing application that would show how to preserve privacy in decentralized ciphertext policy attribute based access control. The system was set up to allow for independent authority participation, secure key management, encrypted file storage, and controlled user access. The system is implemented using JAVA based environment and includes various functional modules such as registration, authorization, key generation, protection of files and their secure retrieval. The prototype is designed based on distributed model of running architecture, access permissions are controlled by attribute-based policies and protected by ciphertext-policy methods . The planned deployment was an application level environment, providing secure interaction between users, authorities and encrypted storage resources. Table 2 summarizes the implementation specifications used for the created framework.

"Table 2. Implementation Environment"

Parameter	Specification
Development Platform	Java Development Environment
Programming Language	Java
Architecture	Decentralized
Security Model	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)
Application Type	Secure File Sharing
Key Management	Independent Authority-Based
Access Control	Attribute-Based Authorization
Storage Type	Encrypted File Storage
Implemented Modules	Registration, Authorization, Key Generation, File Upload, Encryption, Decryption
Deployment Environment	Application-Level Prototype

IV. Experimental Results

A) Functional Validation

To ensure the successful implementation of the developed modules and to validate secure end-to-end operation of the built prototype, the functional validation of the suggested privacy-preserving decentralized CP-ABE framework was performed. The validation procedure was developed to test whether the access process was successfully initiated, the key management was decentralized, the file handling was secure and the data retrieval was controlled. The workflow deployed showed that authorized users were able to seek access and get the necessary authorization credentials, upload protected content, and retrieve encrypted information under pre-defined access circumstances. The system's secure decryption was also confirmed, with access only granted following verification and authorization. The execution outputs of the representative key generation, upload of secure file and successful decryption of file are shown in Fig. 3, Fig. 4 and Fig. 5 respectively. Table 3 shows the outcomes of the functional verification of the implemented modules.

"Table 3. Functional Verification Results"

Operation	Expected Outcome	Observed Outcome	Status
Key Generation	Generate and assign authorization keys	Public and private keys generated successfully	Successful
Access Request	Submit user request for protected resource	Request created and processed successfully	Successful
File Upload	Store protected file securely	File uploaded into encrypted storage	Successful
File Retrieval	Retrieve encrypted file after authorization	Authorized retrieval completed	Successful
Decryption	Recover original content after validation	File decrypted and accessed successfully	Successful

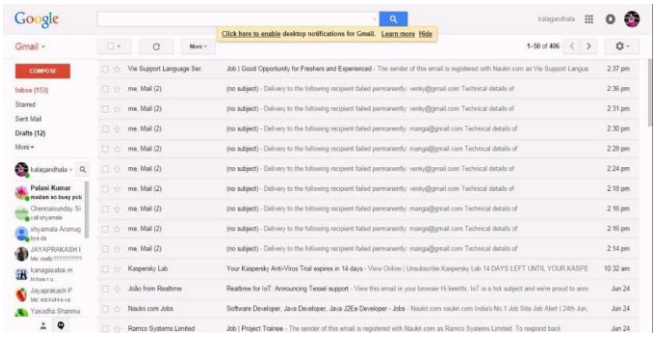


Fig.3 Key Generation Interface

Fig.4 Secure File Upload

Fig.5 Successful File Decryption

B) Privacy and Security Discussion

The proposed system is a privacy-preserving decentralized CP-ABE system, which has some conceptual improvements enabling securing access to data and managing data confidentiality in distributed environment. One of the key benefits of the framework is its ability to ensure that the privacy of the users is not violated with regards to authorization and access control operations. The system does not reveal the user identities but instead checks attributes, so that less user data is exposed during interaction with the system.

In addition the framework improves security by maintaining attribute privacy in all phases of access control. Information about the user may be revealed in user attributes. Minimizing unwarranted disclosure lowers the probability of inappropriate profiling and attribute inference. Further, the GID association mechanism gives safe user differentiation without exposing identities in credential issuing and verification processes.

The proposed architecture employs decentralized authority participation to decrease the trust concentration, thereby facilitating operational flexibility as opposed to traditional architectures that rely on centralized authority control. Independent authority management means that authorities can manage keys and authorize securely and without having to coordinate a lot with each other. This means that there is no central authority to rely on, no limitations of centralized control.

The proposed framework also introduces a mechanism for controlled access management where policy based authorization is used to ensure that the resources are encrypted to only be accessible to those users who have been authorized to access it by the policies set. The framework intertwines privacy-conscious permission and decentralized participation to limit unauthorized access attempts and minimize the chances of data leakage during storage, authorization, and retrieval. Together these features contribute to improving secure and private encrypted data communication environments.

C) Comparative Discussion

In order to understand the improvements in the concept over the current centralized attribute-based access systems,

two categories of ABE systems were compared to the proposed decentralized CP-ABE system with respect to architectural and privacy aspects. It's not about performance, it's about authority management, privacy protection, access flexibility and preservation of confidentiality. This is more than what is offered by current methods, as the suggested system alleviates the centralized dependency and boosts the privacy-invulnerable authorisation as mentioned in Table 4.

Table 4. Conceptual Comparison

Feature	Existing Approaches	Proposed Framework
Central Authority	Frequently required for initialization and management	Not required; authorities operate independently
GID Protection	Limited or partially protected	Supports privacy-preserving identifier management
Attribute Privacy	User attributes may be exposed during authorization	Sensitive attributes remain confidential
Authority Independence	Requires coordination among authorities	Supports independent authority participation
Flexible Access Control	Restricted policy flexibility	Attribute-driven policy-based access control

The comparison demonstrates that the traditional methods often need central coordination and information about identity is shared in the permission process. Previous models improved the level of encrypted access control, but the level of protection of identities and attribute information is limited. Rather, the recommended approach is to emphasize privacy protection: to keep authorities independent of each other and to reduce unnecessary exposure of information in access validation. The decentralized participation with privacy-aware permission further increases the controlled access management and lessens the chances of identity inference and information leakage. The proposed framework is shown to be a flexible and privacy-oriented approach for an encrypted data sharing environment that is safe and secure.

V. Conclusion

We introduced a novel safe data sharing and access control system in distributed systems based on PPDCP-ABE that can preserve privacy for data sharing. While recent attribute based encryption schemes have improved on the confidentiality and policy based authorization, the centralized dependency, identity exposure and attribute privacy are still issues in secure information sharing. Therefore the proposed system proposed a decentralized access control system, where many authorities can take part in the system in an autonomous manner without central coordination. The framework employs attribute-based authorization and privacy-aware key distribution to ensure controlled access while protecting sensitive information belonging to the users. Also GID was utilized for safe authorization without revealing the user identity at the time of the operation of access. The prototype implementation demonstrates that files may be secured by authorisation, encryption, storing and limited decryption. Overall, the proposed solution contributes towards better privacy preservation, minimizing trust concentration, supporting authority independence, and more secure encrypted data sharing environments by means of decentralized access management.

Future Enhancements

Future work should be directed towards increasing security assurances and deploying in large-scale distributed settings. There are several potential areas of further development such as a secure and fully realized implementation of privacy-preserving CP-ABE, access policy protection techniques, integration with cloud platform, and formal validation of security to enhance confidentiality, scalability and real world acceptance.

References

[1] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. Au, "PPDCP-ABE: Privacy-preserving decentralized ciphertext-policy attribute-based encryption," in *Proc. ESORICS*, vol. 8713, Lecture Notes in Computer Science, Springer, Switzerland, pp. 73–90, 2014.

[2] P. Bichsel, J. Camenisch, T. Gross, and V. Shoup, "Anonymous credentials on a standard Java card," in *Proc. ACM CCS*, pp. 600–610, 2009.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, vol. 3494, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 457–473, 2005.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security and Privacy*, pp. 321–334, 2007.

[5] L. Cheung and C. Newport, "Provably secure ciphertext-policy attribute-based encryption," in *Proc. ACM CCS*, pp. 456–465, 2007.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM CCS*, pp. 89–98, 2006.

[7] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM CCS*, pp. 195–203, 2007.

[8] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and hierarchical inner product encryption," in *Proc. EUROCRYPT*, vol. 6110, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 62–91, 2010.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. PKC*, vol. 6571, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 53–70, 2011.

[10] M. Chase, "Multi-authority attribute-based encryption," in *Proc. TCC*, vol. 4392, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 515–534, 2007.

[11] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. ACM CCS*, pp. 121–130, 2009.

[12] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 11, pp. 2150–2162, 2012.

[13] H. Qian, J. Li, and Y. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in *Proc. ICICS*, vol. 8233, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 363–372, 2013.

[14] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proc. ASIACCS*, pp. 386–390, 2011.

[15] J. Herranz, F. Laguillaumie, and C. Rafols, "Constant size ciphertexts in threshold attribute-based encryption," in *Proc. PKC*, vol. 6056, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 19–34, 2010.

[16] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi-authority attribute-based encryption without a central authority," in *Proc. INDOCRYPT*, vol. 5365, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 426–436, 2008.

[17] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *Proc. EUROCRYPT*, vol. 1592, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 295–310, 1999.

[18] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DSS signatures," in *Proc. EUROCRYPT*, vol. 1070, Lecture Notes in Computer Science, Springer, Heidelberg, pp. 354–371, 1996.