International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 5, ISSN No. 2455-2143, Pages 126-131
Published Online September 2022 in IJEAST (http://www.ijeast.com)

ATTRIBUTE-BASED ENCRYPTION SCHEMES FOR BOTH USERSAND CLOUD SERVER

Rajeshwari Gudlanur
PG Student, Department of CSE,
Akshaya Institute of Technology, Tumkur, Karnataka
Visvesvaraya Technological University,
Belagavi, Karnataka, India

Rakesh S.
Assistant Professor, Dept of CSE,
Akshaya Institute of Technology, Tumkur, Karnataka
Visvesvaraya Technological University,
Belagavi, Karnataka, India

Abstract— **To reduce the operator's cost of decryption and secure the sensitive data from an un trusted party, we have an approach to outsourcing the decipherment of the attribute- based encryption (ABE) scheme to the cloud server. The cloud server requires repeating the process of outsourced decipherment facility of the same coded text for different users. Green computing is the environment of careful and reusable employ of methods. This particular scheme can decrease its price needs by obtaining its performance and enhancing resource management and services. The technique is inefficient. To extend the explanation of the recyclable technique of methods for the cloud server, here we have a new approach to decrease t h e total upstairs of the cloud server when many operators fulfilling this scheme require the outsourced decipherments for the similar coded text also reducing the decryption calculation price for operators. Compared with the existing previous methods, our entire limitations of the cloud server is independent of the user numbers who will be satisfied with this scheme and request this decipherment process.**

Keywords: **Green cloud computing, attribute-based encryption, outsourced decryption, cloud server, recyclable utilization, bilinear maps.**

I. INTRODUCTION

Cloud computing makes it possible for users to access user-oriented IT services. The enormous storage space and powerful computer power are the two key profits of cloud computing. Nowadays, thanks to the development of cloud computing, individuals and trades can save their photos, contacts, and other material on cloud servers. Meanwhile, individuals or businesses use powerful computational power as well. Many applications are proposed for cloud computing to make people's standard of living more convenient.

While cloud operators are solely seen as "devices" that takes input and display output, on the one side, cloud users can save money by subcontracting theirdata space or processing to the cloud servers. On the other side, subsequently, a user cannot control their own data, and how to safeguard users' privacy may be a major concern in both academia and business.

Thus, a series of security concerns are considered, including keyword searching, outsourcing verification, outsourcing computation, and remote auditing. The proposed system, a changeable and best access structure scheme, has emerged as one of the most widespread theories to be explored in cloud computing, despite the fact that numerous cryptographic techniques and skills were suggested.

An expanded version of the identity-based encryption concept was considered when developing the ABE that Sahai and Waters presented (IBE). Aside from broadcast encryption, the one-to-many encryption approach is effective.

Recently, two different categories of ABE systems were characterized in accord with the implementation of access control policies,

- key-policy ABE (KP-ABE)
- ciphertext-policy ABE (CP-ABE)

The decryption cost of various ABE systems is asignificant drawback, too. Because the difficulty of the access policy linearly increases with the user's decryption cost as well as the length of the ciphertext. It has grown to be a significant barrier for many cloud computing applications, including those for wireless sensors and smartphones.

In demand to decrease the calculation price of the ABE's decipherment process and make benefit from the high processing capabilities of the cloud server.

An operator can finish a lot of computations in their scheme by paying a little fee to decrypt cipher text using a cloud server. The cloud server calculates a delegate transform key and the encrypted text and generates an altered cipher text. The user can then recover the related original text by performing a "decipherment" method. The ABE-OD method used during the outsourcing process was unable to divulge any information regarding the plaintext due to security concerns.

A. However, they failed to address two additional issues in ABE-OD plan. The first one is that it is very difficult to ensure updated encrypted text accuracy. The method also increases the consultant's overhead because it must first generate the operator's secret key before producing the operator's conversion key. This results in the scheme not being fine-grained for the user (the secret key cannot be utilized anymore).

II. LITERATURE SURVEY

1) J. Yu, K. Ren, and C. Wang, ''Enabling cloud storage auditing with verifiable outsourcing of key updates,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun.

In many network security applications, key-exposure resistance has long been a crucial concern for comprehensive cyber defense. Recently, solutions to the major exposure issue within the auditing of cloud storage have been put out and researched. Existing solutions to the problem all call on the client to update his secret keys on a regular basis This may inescapably result in new local limits for the client, particularly for devices with limited computational power, such mobile phones. We focus on how to present a novel paradigm termed cloud storage auditing with verifiable outsourcing of key updates and form key changes as clear as feasible for the user in this research. The client's burden with key updates will be reduced in this paradigm by securely delegating key changes to a reliable third party. For instance, we utilize the third- party auditor (TPA), designate it as the authorizing team in our situation, and hold it accountable for both thestorage auditing.

Y. Fan, Y. Liao, F. Li, S. Zhou, and G. Zhang, ''Identity-based auditing for shared cloud data with efficient and secure sensitive information hiding,'' IEEE Access, vol. 7, pp. 114246–114260.

With the introduction of cloud computing, information exchange has proliferated, advancing research, particularly in the areas of advanced technical fields. It provides an id-based log system for public cloud information with a safety mechanism to protect delicate information so as to deal with this information concealment, and effectively audit joint information. This proposal's approach permits users to converse openly with researchers while safeguarding private information from both the cloud and those researchers. An extensive security analysis serves as additional evidence of the suggested scheme's high level of protection. Performance evaluation and experimental results show that, due to our unique approach to concealing critical information and streamlining the signature algorithm, our strategy is substantially more efficient than the earlier system. Our system provides the following enticing qualities and benefits over the current method for ensuring the integrity of shared data that conceals critical information. Prior attempts to develop a safe system to thwart malicious managers were unsuccessful, to start with. We close this gap while defending the accuracy and validity of the sent data. Second, our approach develops a different system model that can manage high parallelism and enormous amounts of information in the actual world.

Q. Su, J. Yu, C. Tian, H. Zhang, and R. Hao, ''How to securely outsource the inversion modulo a large composite number,'' J. Syst. Softw., vol. 129, pp. 26–34, Jul. 2017.

Explore the safest outsourcing options for inversion modulo large complex integers. We need to develop the first exact outsourced formula for modulo inversion of large composite numbers. With probability 1, the result can be verified to be accurate. The difficulty of the client's calculation drops from O(l3) to O (l2). Define the tight safety proofs and the formal idea of accuracy. Segmental inversion is one of the utmost fundamental operations in algorithmic number theory. This operation is particularly inefficient for cryptosystems, since the modulus is often a large number. It is unreasonable to expect computing hardware, like smart cards and gadgets, to do such a inefficient calculation. The focus of this research is on the protected outsourcing of inversion modulo a big composite integer. We create a safe subcontracting approach for the client's inversion modulo a big composite number with two known prime components using the Chinese Remainder Theorem (CRT). Our solution secures the modulus'sprivacy in addition to the number's and its modular inversion's confidentiality. The outcome can be independently confirmed to be accurate with probability 1. A l-bit modulus typically has an O modular inversion complexity (l3). Our approach lowers the client side complexity to O by utilizing the cloud (l2). Furthermore, we use the paradigm of a two-untrusted application with one malicious component to show the security of our technique (one-malicious model). We run various tests to show the reliability and applicability of our suggested algorithm. In the appendix, we demonstrate how our suggested technique can be expanded upon and utilised in the RSA algorithm's secret key generation on devices with limited resources.

Y. Liao, Y. He, F. Li, and S. Zhou, ''Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement,'' Comput. Standards Inter., vol. 56, pp. 101–106, Feb. 2018.

By analyzing a protocol that was published in above shown paper and producing the outputs that are displayed below, this work contributes. First, we call attention to the security and design flaws in the protocol. We then improve their protocol. The efficiency and safety of our modified protocol are then assessed. One of the most popular ways to offer payment facilities to businesses and economic institutions utilizing handheld devices like mobile phones and iPads is through mobile payments. However, mobile devices can't perform large-scale computing because of their limited capabilities. The secure outsourcing of some mobile payment processing to a shaky cloud server is therefore preferred. An online payment system with outsourced verification on an unreliable cloud server has been introduced by Qin et al. In this paper, we first show two issues with their protocol: the first is an unreasonable construction that makes it impossible to implement their protocol; The second is a collusion attack that compromises the security of their protocol's verification during the outsourced verification phase between users and an unreliable cloud server. After that, we enhance their protocol and assess its security.

D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,''Public key encryption with keyword search,'' in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., 2004, pp. 506–522.

These persons investigated the difficulty of employing a public key technique to hunt encoded information. Consider the scenario in which user Bob sends user Alice an email that is encrypted using public key. A mail gateway must ascertain whether the mail comprises the word "urgent" in order to route it properly. Another side, is reluctant to grant the gateway access to all of the encryption keys for her messages. We develop a technique that allows Alice to give the gateway a key so that the gateway can figure out whether the term "urgent" is a keyword in an mail without knowing anything else about the mail. The term "public-key cryptography by keyword search" is used to describe this method. Another example is a mail server that stores a range of emails that other users have freely encrypted for Alice. With the help of our technology, Alice can provide her mail server with a key that allows her to identify all emails containing a certain term, but she does not know what that key is. We present the concept of public key encryption and offer various structures using a keyword search.

A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Proc. 24th Int. Conf. Adv. Cryptal., 2005, pp. 457–473.

Identity-based encryption An identity is seen in Fuzzy IBE as a group of defining characteristics. Only if ID and 0 are close, the fuzzy IBE approach can use ID's private key to decrypt the ciphertext encrypted with ID 0, as indicated by the distance metric "Set Overlap". It is precisely the fault- tolerance property of the fuzzy IBE scheme that permits the use of biometric IDs, which by their very nature will always contain some noise when sampled. To enable encryption using biometric inputs as identity, a fuzzy IBE technique can be utilized. Furthermore, we show that Fuzzy-IBE is appropriate for applications that use "attribute-based encryption. Here, we describe two fuzzy IBE scheme structures. Under a number of (fuzzy) identity-defining criteria, our work can be seen as an Identity-Based Encryption of a communication. Our IBE strategies are resistant to mistakes and safe from collusion attacks. Additionally, the central component of our system does not employ random oracles. We use the Selective-ID security concept to demonstrate the integrity of our schemes.

III. ISSUES IN THE EXISTING SYSTEM

Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE was proposed. Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang et al. proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE. Wan et al. proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A cipher text policy hierarchical ABE scheme with short ciphertext is also studied. In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

IV. PROPOSED SYSTEM

The GHW method to construct an ABE-OD scheme called verifiable outsourced decryption of ABE (ABE-VOD), which can verify the transformed ciphertext's correctness by a proxy or the cloud server. A random message and a plaintext are encrypted and meanwhile generated a commitment by the data owner in their ABE-VOD scheme. While the data receiver can make use of her/his private key to create a retrieving key and a transformation key which is utilized to produce a transformed ciphertext. In their decryption algorithm or outsourced decryption algorithm, the commitment is to make use of checking the generated

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 5, ISSN No. 2455-2143, Pages 126-131
Published Online September 2022 in IJEAST (http://www.ijeast.com)

transformed ciphertext's correctness. When the attributes set meets the ciphertext's access structure, the user is able to verify the transformed ciphertext's correctness. The model of their ABE-OD is described in

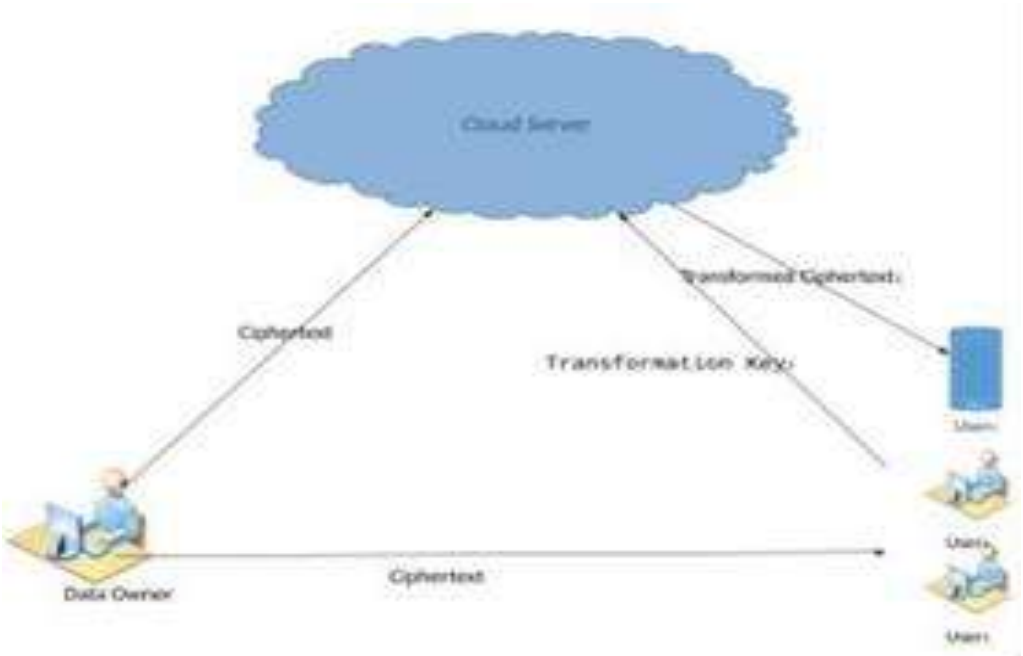
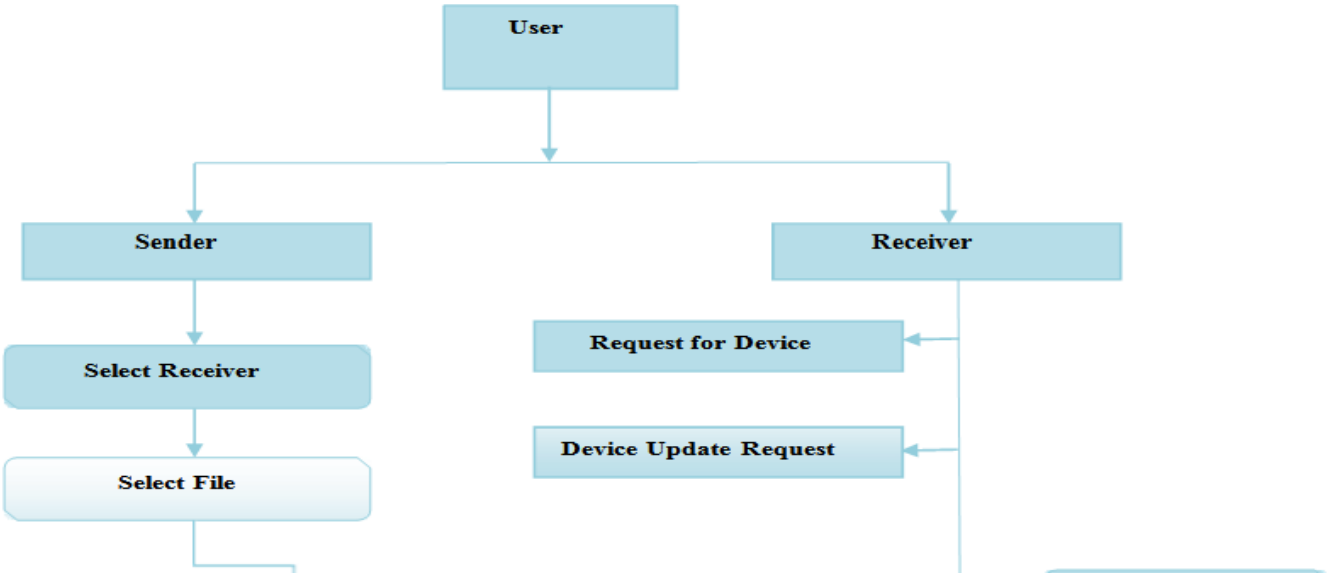


Figure 1. Architecture for ABE-OD

FIGURE 1. Subsequently, relying on distinct scenarios or different correctness- checking methods, several ABE-VOD schemes were presented , while all these schemes used the GHW skill to design the outsourced decryption. Although Qin et al. and Zhao and Wang also put forward ABE-VOD schemes, they required the authority to produce the transformation key. Xu et al. constructed an ABE-VOD scheme from multilinear map that is secure based on k-multilinear Decisional Diffie-Hellman problem. However, Hu and Jia showed that construction of the multilinear map is not secure.

V. SYSTEM DESIGN



International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 5, ISSN No. 2455-2143, Pages 126-131
Published Online September 2022 in IJEAST (http://www.ijeast.com)

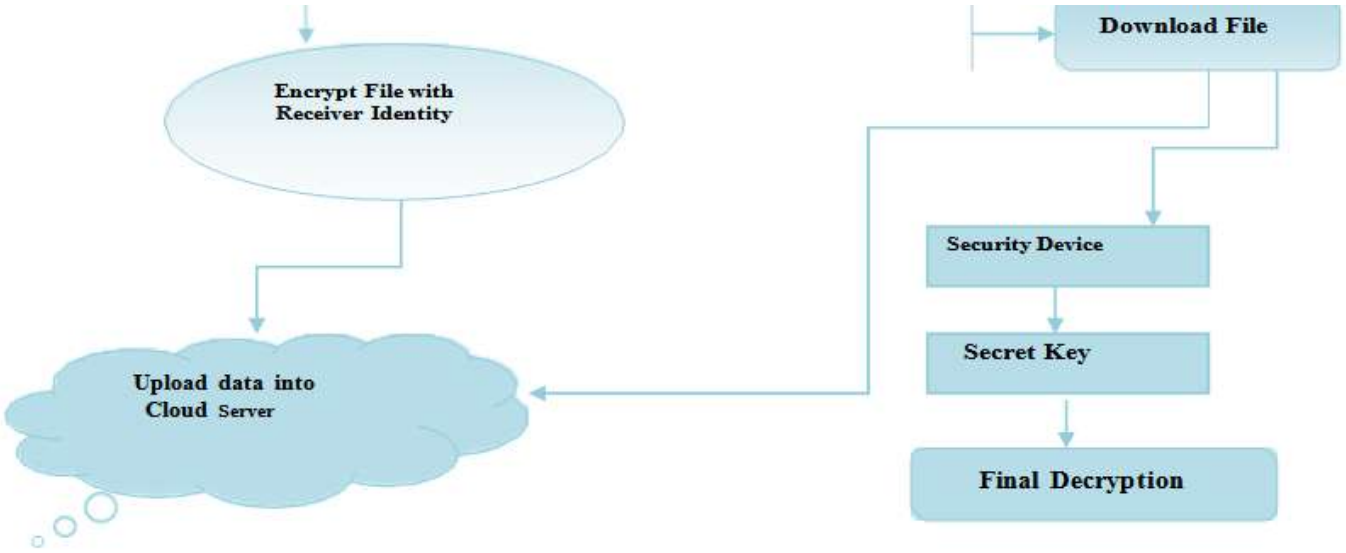


Figure 2. System Architectural Diagram

System Architecture, Big systems are broken down into smaller and smaller systems, that provide some services or handles some tasks. System Architecture deals with the design process description of the subsystems and their control.

A basic structural model is designed for a system. Major modules of the system are identified and communication between these modules are also established. System architectural diagram for the software is given in the diagram 2.

The diagram shown in the figure 2 represents the Sender and Receiver mechanism. The Sender uploads the file using Receiver identity like using EmailId and the Receiver then downloads the file from the cloud.

Functional Description of the Modules The functionality of each module and description of each module is explained in this section. The input required and output generated for the modules are explained. The two main modules in the system are Sender and Receiver.

Sender Module

This module is responsible for Registration (Setup Phase), Secret Key Generation, KDC Request and then File Uploading to the Amazon Cloud Server.

Registration:

- **Functionality :** Sender details are registered
- **Input :** EmailId, Phone Number, Username, Password
- **Output :** Upon registering, successful message is displayed and secret key is sent to the Receiver EmailId

Implementation

This system has some advantages that createit particularly appropriate for information distribution. For instance, it is highly flexible and allows information owners to permit information retrieval based on information consumers instead of, a list of usernames and it verifies information integrity.

Specifically, the proposed scheme creates a content key and encrypts media elements with the particular keys, and then constructs Content Key Cipher text (CT). Operators can decipher the Content Key Cipher text. The content keys can be deciphered using some conventional algorithms.

In this project, attributes are used to define an operator's identifications, and a party encoding data controls a policy thatwhich user can decipher.

The scheme permits for a new kind of enciphered retrieval control in which the operator's secret keys are stated by a group of attributes and a party coding data can state a proposal over these attributes specifying who are able to decipher.

In this project, with fixed-size decipherment keys regardless ofthe attribute numbers.

The project contains four different module units: service provider, authority, data owner, and user. In proposed scheme, if we think that the information owner takes n files with n retrieval levels and A ={a1,..., an }is common in cloud computing. At this point, a1 is the uppermost hierarchy and an is the lowermost hierarchy. If an operator can decipher a1, the operator can also decipher a2,…..,an .

1. Authority: fully trustable unit and takes operator registration in cloud computing. And it can also run some operations Setup1 and KeyGen1.
2. Cloud Service Provider (CSP): semi-trustable unit it can fairly do the allotted work and yield exact output. This project offers encrypted text space and some other services.

3. Data Owner: It contains extensive information that needs to be kept public in cloud systems. In the schema, objects are responsible for defining access structures, performing cryptographic operations, and uploading cipher texts to service providers.

VI. REFERENCE

[1] J. Yu, K. Ren, and C. Wang, ''Enabling cloud storage auditing with verifiable outsourcing of key updates,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375,Jun. 2016.

[2] Y. Fan, Y. Liao, F. Li, S. Zhou, and G. Zhang, ''Identity- based auditing for shared cloud data with efficient and secure sensitive information hiding,'' IEEE Access, vol. 7, pp. 114246–114260, 2019, doi: 10.1109/ access.2019.2932430.

[3] Q. Su, J. Yu, C. Tian, H. Zhang, and R. Hao, ''How to securely outsource the inversion modulo a large compositenumber,'' J. Syst. Softw., vol. 129, pp. 26–34, Jul. 2017.

[4] Y. Liao, Y. He, F. Li, and S. Zhou, ''Analysis of a mobilepayment protocol with outsourced verification in cloud server and the improvement,'' Comput. Standards Inter., vol. 56, pp.101–106, Feb. 2018.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ''Public key encryption with keyword search,'' in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., 2004, pp.506–522.

[6] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Proc. 24th Int. Conf. Adv. Cryptol., 2005, pp.457–473.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute-based encryption for fine-grained access control ofencrypted data,'' in Proc. 13th ACM Conf. Comput. Commun. Secur.-CCS, Alexandria, VA, USA, Oct./Nov. 2006, pp. 89– 98.

[8] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext- policy attribute-based encryption,'' in Proc. IEEE Symp. Secur. Privacy (SP), Berkeley, CA, USA, May 2007, pp. 321–334.

[9] M. Green, S. Hohenberger, and B. Waters, ''Outsourcingthe decryption of ABE ciphertexts,'' in Proc. 20th USENIX Conf. Secur., San Francisco, CA, USA, Aug. 2011, p. 34.

[10] J. Lai, R. H. Deng, C. Guan, and J. Weng, ''Attribute- based encryption with verifiable outsourced decryption,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.