iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

ATTRIBUTE-BASED ENCRYPTION USING KEY EXPOSURE WITH VERIFIED OUTSOURCED DECRYPTION IN CLOUD

S. PARIMALA
MCA Student, Department of Computer Applications, Sri Muthukumaran Institute of Technology
K. KULUNTHAN
Assistant Professor, Department of Computer Applications, Sri Muthukumaran Institute of Technology

ABSTRACT
Attribute-based encryption (ABE) with outsourced decoding not as it were empowering fine-grained sharing of scrambled information, but too overcomes the proficiency downside (in terms of cipher content estimate and decoding fetched) of the standard ABE plans. In specific, an ABE plot with outsourced decoding permits a third party (e.g., a cloud server) to change an ABE cipher content into a (brief) El Gamal-type cipher content utilizing a open change key given by a client so that the last mentioned can be unscrambled much more productively than the previous by the client. In any case, a inadequacy of the unique outsourced ABE conspire is that the rightness of the cloud server's change cannot be confirmed by the client. That is, a conclusion client seems be cheated into tolerating a off-base or perniciously changed yield. In this paper, we to begin with formalize a security show of ABE with unquestionable outsourced decoding by presenting a confirmation key in the yield of the encryption calculation. At that point, we show an approach to change over any ABE conspire with outsourced decoding into an ABE conspire with irrefutable outsourced unscrambling. The unused approach is basic, common, and nearly ideal. Compared with the unique outsourced ABE, our unquestionable outsourced ABE not one or the other increments the user's and the cloud server's computation costs but a few nondominant operations (e.g., hash computations), nor grows the cipher content estimate but including a hash esteem (which is <20 byte for 80-bit security level). We appear a concrete development based on Green et al.'s cipher text-policy ABE conspire with outsourced decoding, and give a point-by-point execution assessment to illustrate the points of interest of our approach.

Keywords
Attributed-based encryption, data sharing, decryption outsourcing, verifiability.

I. INTRODUCTION

Cloud computing is a revolutionary computing fashion, by which computing coffers are handed stoutly via Internet and the data storehouse and calculation are outsourced to someone or some party in a 'Cloud'. It greatly attracts attention and interest from both academia and assiduity due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the stylish of our knowledge. First of all, data confidentiality should be guaranteed. The data sequestration isn't only about the data contents. Since the most seductive part of the Cloud computing is the calculation outsourcing, it's far beyond enough to just conduct an access control. More likely, druggies want to control the boons of data manipulation over other druggies or Cloud waiters. This is because when sensitive information or calculation is outsourced to the Cloud waiters or another stoner, which is out of druggies' control in utmost cases, sequestration pitfalls would rise dramatically because the waiters might immorally check druggies' data and access sensitive information, or other druggies might be suitable to infer sensitive information from the outsourced calculation. thus, not only the access but also the operation should be controlled.

Secondly, particular information (defined by each stoner's attributes set) is at threat because one's identity is authenticated grounded on his information for the purpose of access control (or honor control in this paper). As people are getting more concerned about their identity sequestration these days, the identity sequestration also needs to be defended before the Cloud enters our life. rather, any authority or garçon alone shouldn't know any customer's particular information. Last but not least, the Cloud calculating system should be flexible in the case of security breach in which some part of the system is compromised by bushwhackers. colorful ways have been proposed to cover the data contents sequestration via access control.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

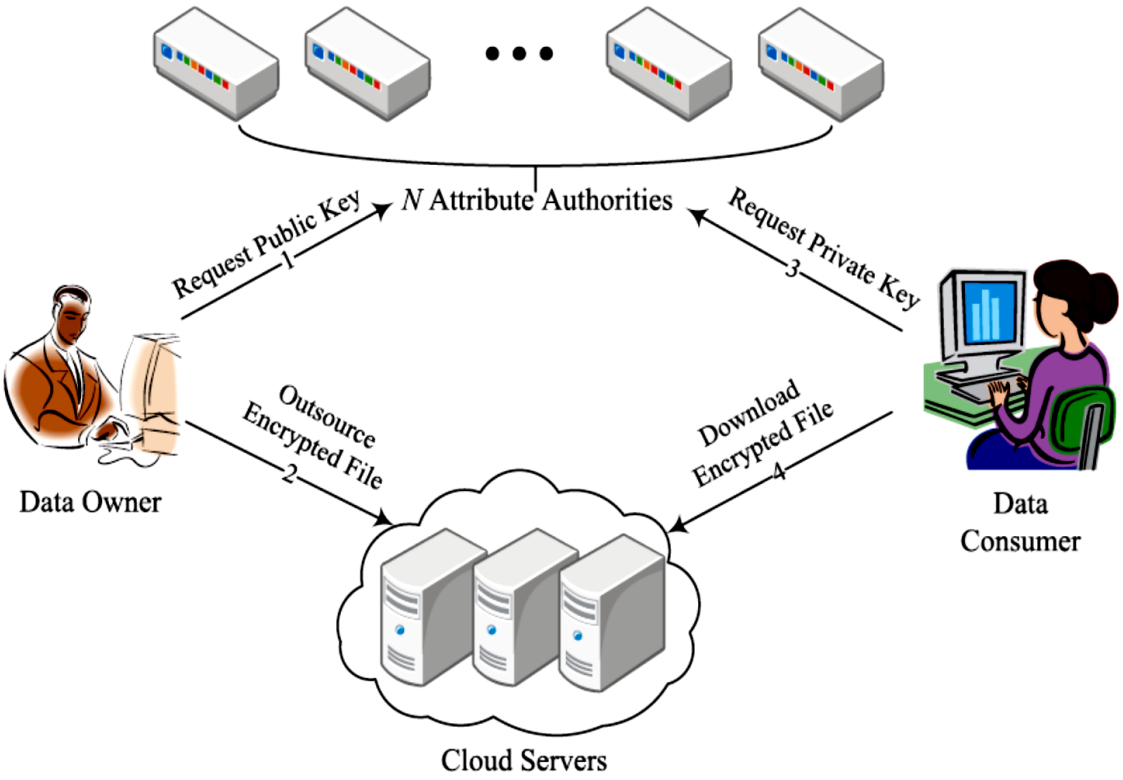


Fig-1. General flow of our scheme.

Identity- grounded encryption (IBE) was first introduced by Shamir [1], in which the sender of a communication can specifies an identity similar that only a receiver with matching identity can decipher it. Many times, latterly, Fuzzy Identity- Grounded Encryption is proposed, which is also known as trait- Grounded Encryption (ABE). In similar encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypters identity has some overlaps with the one specified in the ciphertext. Soon later, more general tree- grounded ABE schemes, crucial- Policy trait- Grounded Encryption (KP-ABE) and Ciphertext- Policy trait Grounded Encryption (CP- ABE) [2], are presented to express more general condition than simple 'imbrication'. They're counterparts to each other in the sense that the decision of encryption policy (who can or cannot decipher the communication) is made by different parties.

II. RELATED WORK

Cloud management is gaining increasing attention due to the importance of ensuring that only authorized users have access to trusted services. The cloud is used to store large amounts of data, much of which is interrelated. Access control must be provided for sensitive information that often affects health, important documents (such as files in Google Docs or Dropbox), and even personal information (such as information in social networks). User-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC) are the three main categories of access control. Users who have access to information are listed in the Access Control List (ACL) of UBAC. This is not practical, considering the number of users in the cloud. Users are classified according to their specific capabilities by RBAC (denoted by [1]). Users with the appropriate role can access data. The system creates a role. For example, an assistant secretary may not only have access to information;

For example, in the above case, both a senior secretary with more than eight years of experience and a teacher with more than ten years of research experience are learning to access information. The advantages and disadvantages of RBAC and ABAC are discussed. Some projects have been completed on cloud ABAC. All these efforts use behaviour-based encryption, cryptographic building blocks (ABE). There are many features that users in ABE can add to their personal identity. ABEs are divided into two broad categories.

In the ABE or KP-ABE key policy, the sender has the right to access the encrypted data (Goyal et al. [3]). Writers whose keys and attributes are removed cannot write normal files. If the message has matching attributes,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

the receiver can decrypt the message by getting the attributes and key from the code character. In the ciphertext rule CP-ABE ([4], [5]), the receiver has a monotonic access pattern with AND, OR and other starting points, and the access rule is a tree with leaves.

III. INTRODUCTION TO ATTRIBUTE-BASED ENCRYPTION (ABE)

In the era of big data, Internet users often choose to upload their personal data to remote cloud servers to reduce local data management and maintenance costs. However, it also inevitably faces many unpredictable security and privacy problems.

We start with Attribute-based encryption (ABE), which is an important reason because it provides the best resources for sharing and searching information. After saving data to the cloud server, the data owner usually needs to do two necessary tasks: one is to search for data, the other is to share data. uses traditional ABE tools to encrypt data and keep data confidential, but restricts the sharing and searching of data. File is encrypted according to a rule, and suppose that there is an encrypted genome sequence donated by anonymous volunteers for scientific research. Information such as. pi can only be obtained from the research team that meets the strategy. The ciphertext is stored on a remote server.

To search for certain encrypted genomic data, a researcher (like Alice) needs to download all the ciphertexts related to the PA decryption policy to the server and then decrypt them locally to complete the search task. When sharing one of her current files with a colleague, Alice needs to download the encrypted file, decrypt it, and re-encrypt it according to the colleague's decryption policy. Another interesting behavior (probably performed by Alice) is sharing content updates for encrypted devices.

Consider encrypted genomic data tagged with the keyword. Alice may choose to change its tag to after sharing with researchers in Lab B. Since traditional ABE cannot support content updates, Alice must update the signatures of all shared ciphertexts herself in order to maintain the confidentiality of the content. Section, because they carry an additional burden of decryption/encryption for Alice, who must be online at all times. As the amount of data searched and shared continues to increase, the cost to data owners will increase.

In addition, the size of the downloaded files creates difficulties for local data management, which actually reduces the efficiency of remote data. Alternatively, a third party can be authorized (remotely) to perform search operations, data re-encryption, and content updates for Alice. However, this requires the party to trust Alice because it has knowledge of the search terms (i.e., what Alice wants to search for) and has given the key to Alice (i.e., knowing the following information).

The leakage of the above information seriously harms the privacy of anonymous individuals, as genomic information may contain sensitive information such as diseases. Hence, this approach is also undesirable due to lack of privacy and confidentiality. From the above discussion, we can see the importance of secure search and sharing of encrypted data in remote cloud storage scenarios

.

IV. PROBLEM FORMULATION

The model, N character management (abbreviated as A), cloud servers, data owners, and user data are four different aspects of our system. Users can be data owners and data users. Since some behaviors involve user personal identification information, authorities are considered to have significant computing power and are under the control of government agencies. Each rule has a decision on one of the N disjoint sets that make up the entire production. As a result, all laws are known only to small objects.

The organization that wants to send encrypted data to the cloud server is called the data owner. They are stored only by cloud servers that are believed to have sufficient storage capacity. Added new information for clients to request a private key from any organization, as they are not sure which organization controls which behaviour. In case the data user requests a private key, the authorities will jointly generate the relevant private key and provide it to the data user. All encrypted files can be downloaded from any Data.

V. PROPOSED ARCHITECTURE

In this paper, we first formalize the ABE security model with external decryption credentials by showin g the credentials in the output of the encryption algorithm. Then, we propose a method to transform the external decryption ABE schemes into external decryption ABE schemes in a new way. Convert the ABE ciphertext to t he (short) El Gamal type ciphertext using the client's public key transformation tool, so that the user can decrypt the latter better than the original.

The new method is simple, versatile and almost perfect. We present a specific model of ciphertext-based policy. Adopt ABE solution for decryption and provide detailed performance data to demonstrate it.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

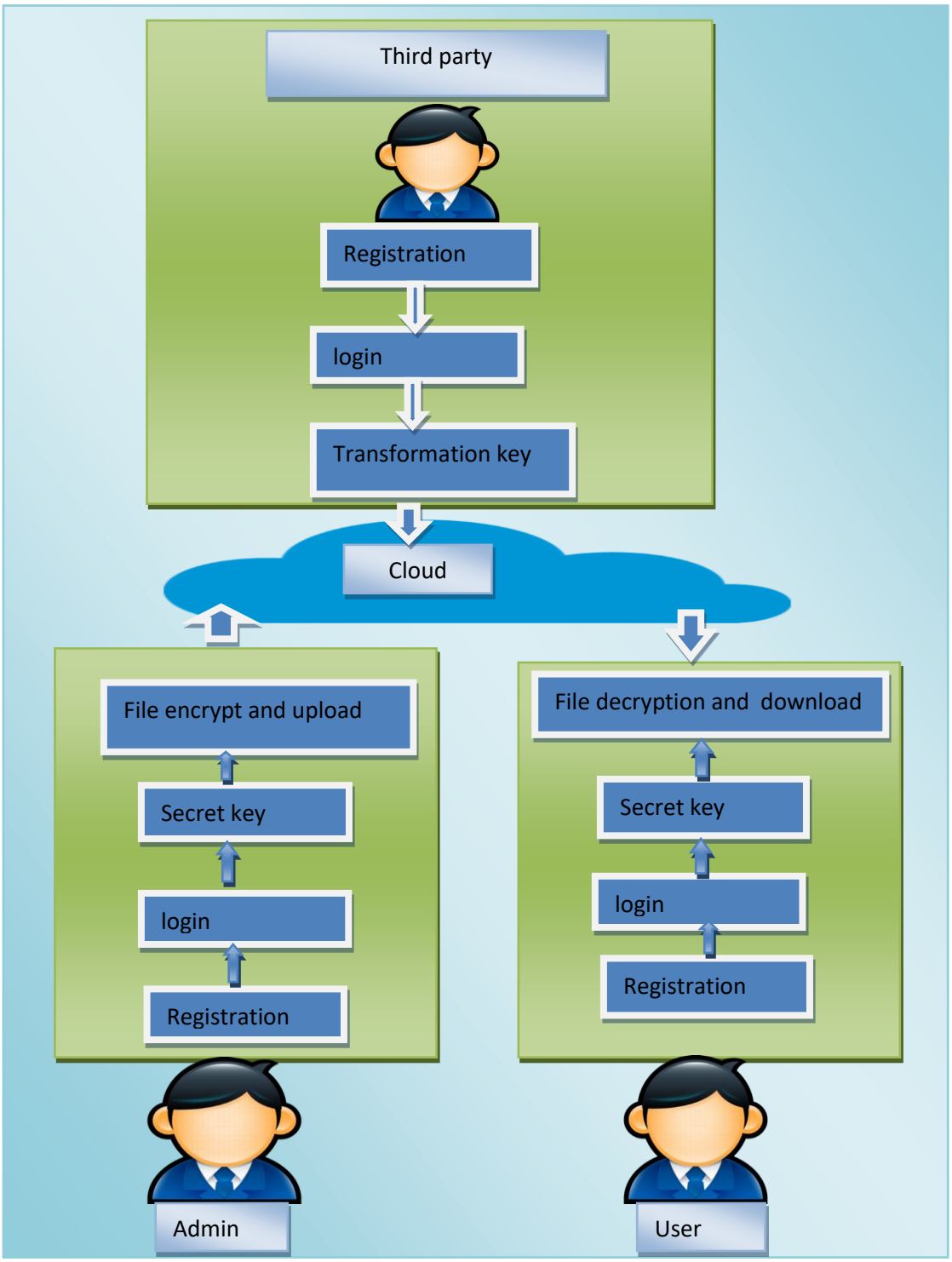


Fig-2. Architecture

ARCHITECTURE OF DATA SECURITY IN CLOUD

A strategy called encryption is prepared at different levels according to the ciphertext level character. Attribute-based encryption (ABE) has many advantages over public key encryption, such as flexible one-to-many encryption that can replace one-to-one encryption.

ABE solutions provide a powerful way to ensure data security and quality control. In the CP-ABE scheme, private keys are tagged with a series of identifiers. The user can only obtain the plaintext when the

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

descriptive process for entering the ciphertext is fulfilled. When the data owner wants to provide data with certain attributes to all users, he can use ABE to encrypt the data, and when the user is satisfied by focusing on some attributes, the user can decrypt the data. The data provider uses standard access in the message. It is difficult to provide detailed access control and reflect the importance of attributes.

To solve this problem, we introduce hierarchical behavior to CP-ABE. The attributes in our scheme are divided into different levels according to their importance in access control. Each user in the system has a hierarchical structure. The data manager encrypts data for users in the system with a special process. The ciphertext has a hierarchical access structure. In order to determine the message, the user behavior in the hierarchy must meet the hierarchical access criteria. The CP-HABE concept can be considered as a generalization of the traditional CP-ABE process where all attributes are at the same level.

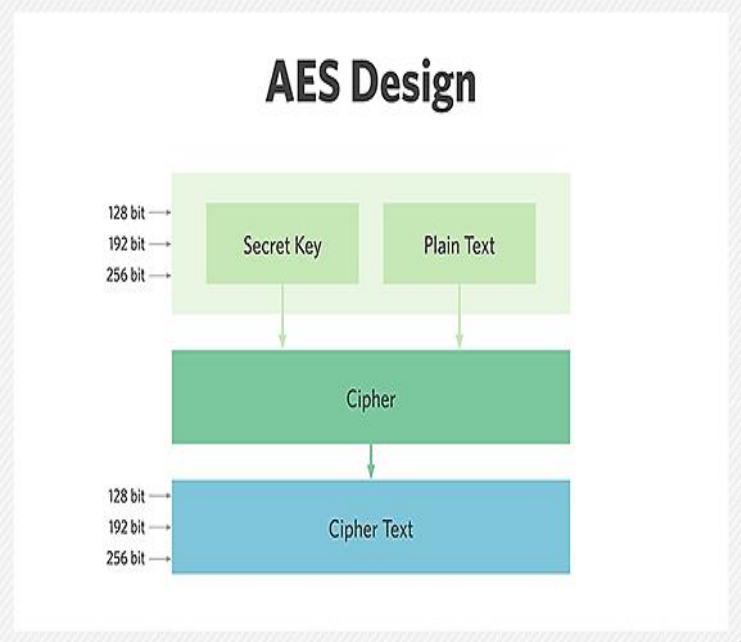


Fig-2. AES

Each cipher uses 128-bit, 192-bit, and 256-bit keys to encrypt and decrypt data in blocks of 128 bits. The Rijndael cipher is designed to accept key sizes and values, but AES does not use these features.

Symmetric (also known as golden key) ciphers use the same golden key for encryption and decryption, so both the sender and the receiver must know and use the same golden key. Any key length is considered sufficient to protect information up to the "Secret" level, and "Top Secret" information requires a key length of 192 bits or 256 bits. There are 10 rounds for a 128-bit key, 12 for a 192-bit key, and 14 for a 256-bit key; each round introduces various operations such as shifting, unshifting, and scrambling words into the final output ciphertext. Section

AES encryption algorithm defines various changes to the data stored in the array. The first step in encryption is to put the information in a single place; The number of rounds is determined by the key length; 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The first change in the Section

AES encryption cipher is to modify the data using the transformation table; The final transformation is a simple exclusive OR (XOR) operation using a different encryption key in each column; longer keys require more processing.

AES has been proven to be a reliable system, and the only effective way to attack AES is to use external attacks to attack vulnerabilities in the implementation or control of product-specific AES-based encryption.

Side-channel attacks exploit flaws in the way the cipher is used, not brute force or theoretical weaknesses in the cipher. A good example is the browser Exploit Against SSL/TLS (BEAST) vulnerability targeting the TLS v1.0 protocol; TLS can use AES to encrypt data, but due to the TLS message disclosure, attackers are able to predict when the encryption process will start the vector blocking.

VI. MODULES

Privacy protection:

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Data servers can be trusted to ensure data confidentiality and enforce legitimate access controls. However, this assumption is not true today because the service shares data across multiple servers with other data owners.

Key generation and file upload:

ABE schemes can be divided into two groups: ciphertext code ABE (CP-ABE) and key code ABE (KP-ABE) [2], depending on whether the code is entered by the ciphertext or the user. In CP-ABE, the access code A is embedded in the ciphertext CT, and the user's key SK is associated with the operation S. The ciphertext CT can be decrypted by SK if and only if f(A,S) = 1 in some cases, the previous function f, i.e. $S \leq A$. In KP-ABE, each ciphertext is associated with a protocol, and each user's private key is associated with the character's access code.

Convert to another file:

The conversion key can be shared publicly with an intermediary called Ciphertext Translation Server (CTS), while the DK private key needs to be kept by the user. The ABE ciphertext is stored in the cloud storage server (CSS). The ciphertext CT stored in CSS is first sent to the CTS CTS using the TK key to convert CT to the simple and short El Gamal type ciphertext (CT_) of the same message, which is not directly decrypted by the user. Therefore, users can save bandwidth and local computation time. In the following, we will use the terms "outsourced decryption ABE" and "outsourced ABE" interchangeably.

Basic Proof:

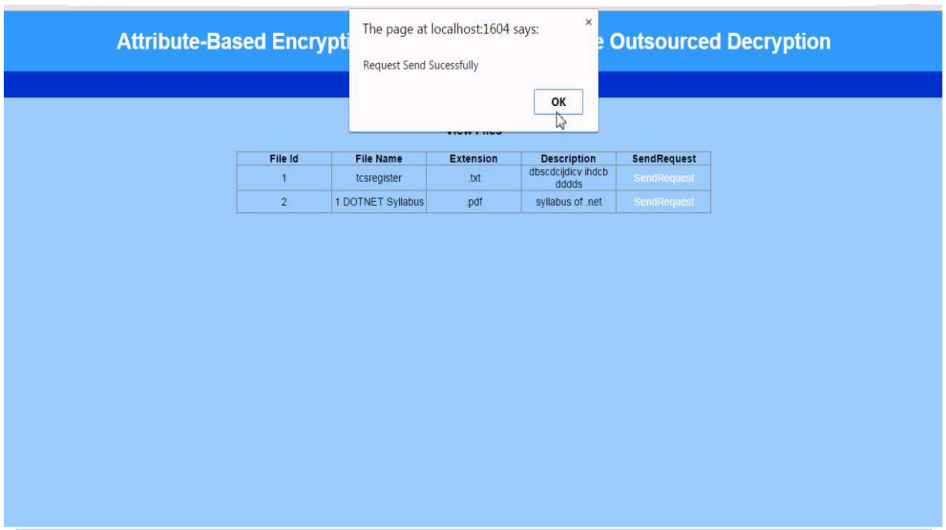
An efficient method to verify the correctness of ciphertext changes that are out of bounds in ABE processes. More specifically, our method is based on an ABE proposal that works in the Key Encapsulation Mechanism (KEM) environment, where the ABE ciphertext encrypts a conversation key.

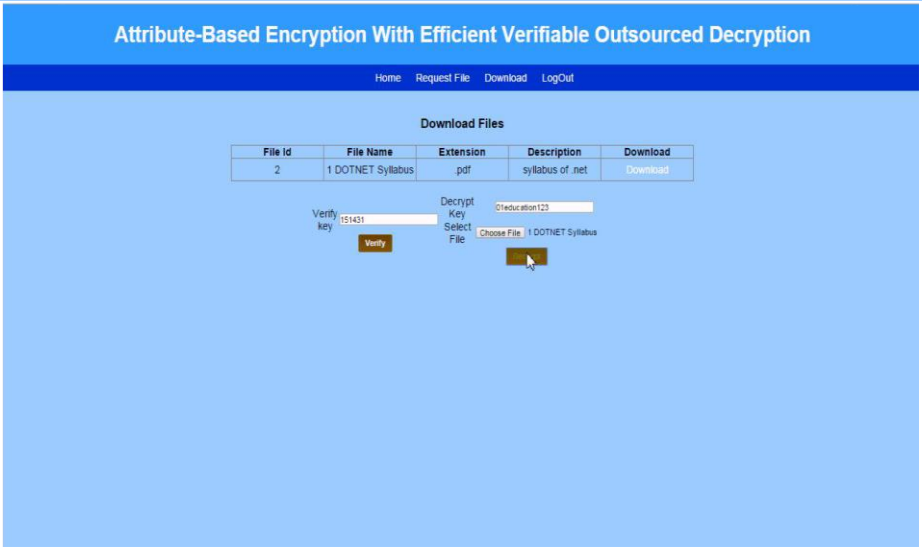
Decrypt and download archive:

We prepare concrete structures with the ABE system and outsourced decryption certificates. Their structure appends regular ciphertexts containing random words and labels (such as real words and random words) to each ciphertext, and requires an original ciphertext that is not transformed by the user in the final decryption step. Compared with Green et al.'s outsourced ABE scheme [8], Lai et al.'s scheme [9] shows significant overhead of both ciphertext size and decryption (see comparison in Table I). In [16], the authors presented an effective method to check the authenticity of outsourced decryption in decentralized systems.

Screen shots

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/





VI. CONCLUSION AND POSSIBLE EXTENSIONS

In this paper, we propose a simple and widely used method to transform an ABE scheme without external decryption proof into an ABE scheme with external decryption proof in a standard model. To verify the effectiveness of the new approach, we present an example of a general approach based on Green et al external CP-ABE scheme, but without the proof. We implemented our example, Green et al. scheme, and Lai et al verifiable external decryption scheme on a PC. Experimental results show that our approach is nearly optimal, as it imposes very little overhead on the analysis in our future work.

VII. REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.
[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio,R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.
[5] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2013, pp. 463–474.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.
[8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.
[9] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.
[10] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011, pp. 386–390.
[11] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in Proc. 31st STOC, 1999, pp. 245–254.
[12] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," Commun. ACM, vol. 28, no. 6, pp. 637–647, 1985.
[13] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," IEEE Trans. Comput., vol. 53, no. 2, pp. 232–240, Feb. 2004.
[14] W. Ren, K. Ren, W. Lou, and Y. Zhang, "Efficient user revocation for privacy-aware PKI," in Proc. ICST, 2008, Art. ID 11.
[15] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.