Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Identity-Based Encryption Transformation Data Sharing in Cloud Assisted Smart Healthcare System

Monisha , Mrs. Anila S.V M.TECH
Department of CSE, Marthandam College of Engineering and Technology, Kuttakuzhi, India

ABSTRACT

With the rapid development of cloud computing, an increasing number of individuals and organizations are sharing data in the public cloud. To protect the privacy of data stored in the cloud, a data owner usually encrypts his data in such a way that certain designated data users can decrypt the data. This raises a serious problem when the encrypted data needs to be shared to more people beyond those initially designated by the data owner. To address this problem, the proposed system introduce and formalize an identity-based encryption transformation (IBET) model by seamlessly integrating two well-established encryption mechanisms, namely identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). In IBET, data users are identified and authorized for data access based on their recognizable identities, which avoids complicated certificate management in usual secure distributed systems. More importantly, IBET provides a transformation mechanism that converts an IBE cipher text into an IBBE cipher text so that a new group of users not specified during the IBE encryption can access the underlying data. It design a concrete IBET scheme based on bilinear groups and prove its security against powerful attacks.

Keywords : Cloud Computing, Data Sharing, Data Privacy, Access Control, Cryptographic Encryption.

I. INTRODUCTION

In recent years, with the technical advance in wireless sensor network, we have witnessed the vigorous development of the Internet of Things (IOT). Featured with instantaneity, universality and easy to deploy, IOT attracts increasing popularity and attentions from the public, and has been widely applied in various fields such as smart transportation, healthcare, smart home, industrial manufacturing and smart grids. In essence,

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

IOT provides an efficient data service mechanism, which enables people to dynamically and accurately monitor an object by using the real-time collected data, this is especially valuable in the field of healthcare. So, it becomes a new developing trend in the healthcare field that build the healthcare system with the IOT. In a typical IOT-oriented healthcare system, the implantable sensor and the wearable sensor collect the real-time health data (including the blood pressure, the heart rate, the breathing rate, and etc.), then forward it to the terminal device owned by the specified doctor. In this way, the doctor can monitor the patient's health precisely in real time, so as to provide the health advice and diagnosis scheme, and to be able to respond to the potential paroxysmal diseases. Usually, the patient can also choose to upload the collected health data to the cloud in addition to being downloaded by his/her doctor, the data can also be used for research purpose by medical institutions, then the patient would be rewarded for the data sharing. However, there is a dilemma lies ahead: If we send and store the data to the cloud in the form of plaintext, then the sensitive data privacy would be easily exposed to the attacker, the unauthorized data users as well as the cloud (the cloud is set to be semi-trusted, and is curious to the stored data). In contrast, if it upload the health data to the cloud in the encrypted form, then it is hard for the authorized data user to distinguish the desired encrypted data from massive ciphertext stored in the cloud. A theoretically possible solution to the dilemma is enabling the data user to download all his/her authorized access ciphertext and decrypt them, but it undoubtedly consumes inestimable heavy computational and storage overheads, thus is obviously impracticable. Fortunately, searchable encryption (SE) was proposed as a feasible and efficient solution. In a typical SE scheme, the data owner selects a keyword from the public keyword dictionary, then generates the cipher text and embeds the selected keyword into the cipher text. In another side, the data user first selects a queried keyword from the dictionary, then generates a trapdoor associated with his/her queried keyword and forwards the it to the cloud. In this way, the cloud can retrieve the corresponding cipher text according to the trapdoor. Inspired by the feature of efficient cipher text retrieval, researches have devoted their efforts to the SE schemes for the healthcare field in recent years. However, the practical healthcare scenarios require the doctor and the medical institution are able to flexibly access the health data from various patients according to the system authorization, while the patient's identity privacy should not be disclosed to doctors and medical institutions, even if they are authorized to access. This seems to be a tough nut, but what is surprising is that attribute-based encryption (ABE) perfectly satisfies the above requirements. ABE regards whether an attribute set satisfies an access structure as the criteria to judge the access authorization of a data user, thus providing one-to-many fine-grained access control. More specifically, ABE schemes are categorized as key-policy ABE (KP-ABE) and cipher text-policy ABE (CPABE) according to their different authorization management: In the application scenario of KP-ABE, the data owner is Labeled with a set

Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

of descriptive attribute set, while the data user is assigned an access structure according to his/her enjoyed service scope. The data user can access the data only if his/her specified access structure satisfies the data owner's attribute set. In contrast, in the application scenario of CP-ABE, the access structure is designed by the data owner himself/herself, he/she can decrypt the cipher text generated by the data owner only if the data owner's attribute set content his/her access structure. Motivated by this, researchers combined ABE and SE to present the novel cryptographic primitive of attribute-based searchable encryption (ABSE), which inherits the traits of cipher text keyword search and fine-grained access control, and is expected to be deployed in the smart healthcare system. However, the exponentiation and the pairing operations in the above ABSE schemes incur heavy computational overheads, this implies that the resource-constrained devices in patient and doctor sides require more time to share and recover the health data, which is obviously unacceptable in the healthcare scenario that emphasizes instantaneity. To accelerate the speed of encryption and decryption, a few latest literatures were published to reduce the computational overheads in online encryption phase and decryption phase with the online/offline encryption and outsourced decryption technology, respectively. However, online/offline encryption just "transfers" the operation of some cipher text components generation to idle time, and does not actually reduce the consumption of computational resources and energy of the sensor. Besides, considering that these implantable and wearable sensors are usually battery-powered, so they have to be charged frequently to supply the expensive energy consumption (some implantable sensors are even non-rechargeable, they would maintain a shorter lifespan).

A. Contributions

In this paper, it try to answer the above question by studying encryption transformation between two different encryption systems. For the first time, it propose a novel notion called identity-based encryption transformation (IBET).It also define the notion (including algorithm definition and security model) of IBET. Then it design a concreteIBET scheme in bilinear groups, which provides the followingattractive features.

- *Identity-Based Data Storage:* Data owner can securely outsource their data to a remote cloud server which is not fully trusted. The data are encrypted and stored inthe server in IBE/IBBE cipher text format so that only the users authorized by the data owners can access them. All users, including data owners and data consumers, are recognized with their unique identities, which avoids the usage of complicated public-key certificates.

- *Cross-Domain Encryption Transformation:* Our IBET scheme achieves a cross-domain encryption transformation which can be viewed as a bridge connecting IBE andIBBE. In particular, a data owner (or an authorized data consumer) can transform the data stored in IBE cipher textformat into the data in IBBE cipher text format, so that a set of users specified by the data owner (or the authorizeddata consumer) can simultaneously access the data.
- *Strong Security Guarantee:* Our IBET scheme achieves astrong security in the sense that: 1) it can deter any unauthorized access to the data stored in the cloud server; 2)it can prevent leakage of some private information (e.g., private key) about the one who authorizes to transform encrypted data; 3) the transformation would not reveal any useful information about the sensitive data.

B.Related Work

Out sourced data protection. Cryptographic encryption methods have been extensively used to secure data outsourcedto clouds. Traditional public-key encryption methods are applied to achieve user-centric access control on outsourced data [4], [5]. Identity-based encryption (IBE) [6] is a promisingcryptographic tool which eliminates trusted certificates for all users. Wei *et al.* [7] exploited IBE to secure data sharing in mobile computing environments. He *et al.* [8] employed IBE to construct a handshake scheme in healthcare socialnetwork to secure data exchanged in patients. Identity-based broadcast encryption (IBBE) [9] extends IBE to support multi-receiver encryption in the sense that a user encrypts a messageonce for multiple intended receivers. In light of such useful feature, Deng *et al.* [10] utilized IBBE in cloud storage systems to allow multiple authorized visitors to access the same outsourced file. To revoke some recipients from the initial receiver set of the IBBE cipher text, a number of revocable IBBE schemes are proposed [11]–[14].

1) Inter-Domain Transformation: Blaze *et al.* [15] first introduced the concept of proxy re-encryption to handle cipher text transformation within an encryption system. With this PRE, a user can transform a cipher text generated under Alice's public key into a cipher text under Bob's public key. Ateniese *et al.* [16] classified PRE into different categories: bidirectional and unidirectional PRE, single-hop and multi- hop PRE, interactive and non-interactive PRE. Many efforts have been made to improve efficiency and security of PRE and most of them focus on unidirectional PRE. Libert and Vergnaud [17] presented the first unidirectional PRE scheme. Cao *et al.* [18] proposed the autonomous path PRE schemeto enable a user to designate a path of preferred authorized visitors to his outsourced data. Guo *et al.* [19] introduced accountability into unidirectional PRE to identify the proxy which abuses its re-encryption keys.

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

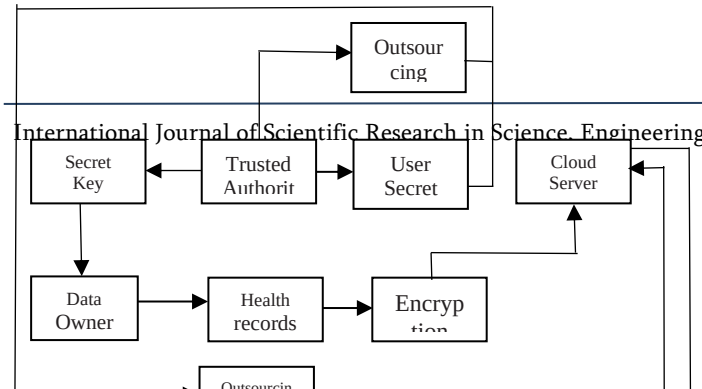
By combining PRE and IBE, Green and Ateniese [20] proposed the first identity-based PRE (IBPRE), which is an extension of PRE in identity-based settings. Chu and Tzeng[21] presented an IBPRE scheme with short ciphertexts and decryption keys, while it is vulnerable to collusion attack, i.e., the coalition of the proxy server and the authorized users could compromise the secret information about data owners. Liang *et al.* [22] overcome this security issue by proposing the cloud-based revocable IBPRE scheme. Thisscheme requires the interaction between data owners and akey generator authority for each transformation, which may result an efficiency problem. Xu *et al.* [23] proposed an IBBE-based PRE scheme by introducing IBBE into PRE. Apart fromIBPRE, there are other extensions of PRE, such as attribute- based PRE [24], [25], time-based PRE [26], function-based PRE [27], etc. However, these PRE schemes mainly provides cipher text transformation in the same encryption system, that is, cipher texts cannot be converted into another format.

2) Cross-Domain Transformation: There are a few schemesachieving cross-domain encryption transformation. Matsuo
[28] linked the traditional public-key encryption and identity- based encryption by allowing to transform a cipher text of public key systems into a cipher text of IBE systems. Mizuno and Doi [29] also proposed a unidirectional PRE scheme that transforms cipher texts of an attribute-based encryption systeminto cipher texts of an IBE system, while requiring users to interact with each other and store additional information for transformation. Recently, Jiang *et al.* [30] proposed a cross- domain encryption switching scheme that connects traditional public-key encryption and identity-based encryption, whileit requires cryptographic certificates for all the users in the public-key encryption system.

SYSTEM MODEL

A. *System Architecture*

The architecture of our IBET system is shown in Fig. 2. An IBET system consists of four types of entities, that is, data owners, data consumers, registry authority (RA) and cloud service provider (CSP). Generally, data owners and dataconsumers are both cloud clients. RA is a trusted party thatis responsible for setting up system, responding to registration requests and issuing public parameters for file outsourcing. CSP has two



Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Fig. 2. System architecture.

major tasks: 1) providing storage services for clients to store outsourced files; 2) providing computation services for clients to transform stored files. In real world,an enterprise or an organization can buy the storage and computation services provided by CSP, and the IT center of the enterprise or the organization plays the role of RA.

Data owners can outsource data to CSP. Specifically, to protect data privacy, data owners can employ IBE encryption mechanism to process data and then outsource the resulting files (data in cipher text format) to CSP. Suppose that a file is the result of IBE encryption for some data (thus the data canbe accessed by only one data consumer). If

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

the corresponding data owner further wants to share the data with more data consumers, he generates an authorization token and sends it toCSP; then CSP can transform the file in IBE cipher text formatinto a file in IBBE cipher text format so that all designated data consumers can decrypt and then access the underlying data. In this way, for the data previously encrypted by IBEand originally accessible to only one data consumer, the data owner can authorize more data consumers to access it.

B. *Threat Model and Security Goals*

An IBET system confronts three types of active attacks. First, cloud clients may impersonate data owners or authorized data consumers to try to access outsourced data, e.g., an employee pretends to be his colleague by using the colleague's device to access CSP. Second, malicious CSP or hackers intruding in cloud servers may search and steal owners' data. Third, CSP may abuse the authorization tokens of data owners to transform encrypted data that are out of the scope ofauthorization. Considering these realistic attacks, we require that a secure IBET system should at least satisfy the followingsecurity goals.

· Data security protection: If data have been encrypted before outsourced, then only the clients holding correct decryption keys can access (these client are also called authorized clients). The encrypted data are unreadable to CSP or unauthorized clients (those having no correct decryption keys).

· Controllable transformation: Only the files specified by the data owner in the authorization token can be transformed by CSP. CSP and other clients cannot cooperatively deduce a valid authorization token in order to transform unspecified files, nor detect sensitive information about the data encrypted in unspecified files.

DEFINITIONS

A. *Framework of IBET System*

Formally, an IBET system consist of six polynomial-time computable algorithms, that is, Setup, Register, Encrypt, Authorize, Transform, and Decrypt.

· Setup$(1^{\lambda}, m)$ (PP, MSK) The system setup algorithm, run by RA, takes as input a security parameter λ and the allowed maximal number m of data consumers
authorized to access the same data. It outputs the public parameter PP for the system and the master secret key MSK for RA itself.

· Register(PP, MSK, ID) SK_{ID} : The registrationalgorithm, run by RA, takes as input the public parameter PP, the master secret key MSK and an identity $ID \in$

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

$\{0,1\}^*$. It outputs a private key SK_{ID}.

· Encrypt(PP, M, ID) CT_{ID} : The encryption algorithm, run by a data owner, takes as input the public parameter PP, the message M to be encrypted and an identity ID. It outputs an IBE cipher text CT_{ID}.

· Authorize(PP, SK_{ID}, S) $TK_{ID\to S}$: The authorization algorithm, run by a data owner with identity ID, takes as input the data owner's private key SK_{ID}, the public parameter PP and the set S of identities of data consumers. It outputs an authorization token $TK_{ID\to S}$.

· Transform$(PP, TK_{ID\to S}, CT_{ID})$ CT_S: The transformation algorithm, run by CSP, takes as input the authorization token $TK_{ID\to S}$, the public parameter PP and the IBE cipher text CT_{ID}. It outputs a transformed (IBBE) cipher text CT_S.

· Decrypt$(PP, CT_{ID}/CT_S, SK_{ID'})$ $M/\perp$: The decryption algorithm, run by a data consumer ID', takes as input the public parameter PP, a private key $SK_{ID'}$ and a cipher text CT_{ID} or CT_S. For CT_{ID}, it outputs the message M if $ID = ID'$ and a false symbol $\perp$ otherwise; for CT_S, it outputs the message M if $ID' \in S$ and a false symbol $\perp$ otherwise.

A secure IBET scheme should be *sound*, that is, if each entity honestly follows the scheme, then any failure would not happen during the scheme running. Formally, for any $(PP, MSK) \leftarrow$ Setup$(1^\lambda, m)$, the following conditions must be satisfied:

· For any IBE cipher text $CT_{ID} \leftarrow$ Encrypt(PP, M, ID) and any private key $SK_{ID'} \leftarrow$ Register(PP, ID', MSK), if $ID = ID'$, then the decryption algorithm Decrypt$(PP, CT_{ID}, SK_{ID'})$ always outputs the plaintext M.

· For any transformed cipher text $CT_S \leftarrow$ Transform$(PP, TK_{ID\to S}, CT_{ID})$, where $TK_{ID\to S} \leftarrow$ Authorize(PP, SK_{ID}, S) and $CT_{ID} \leftarrow$ Encrypt(PP, M, ID), and any private key $SK_{ID'} \leftarrow$ Register(PP, MSK, ID'), if $ID' \in S$, the decryption algorithm Decrypt$(PP, CT_S, SK_{ID'})$ always outputs the plain-

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

text M.

The first condition is straightforward. It means that any encrypted message in IBE cipher text format can only be decrypted by the intended data consumer. The second one is somewhat sophisticated. Its main idea is to define that any properly transformed cipher text (from an IBE cipher text) can be correctly decrypted by all intended data consumers. Thus, we must define what is a properly transformed cipher text and who are the intended data consumers able to decrypt the cipher text.

For a transformed cipher text, the second condition defines that this cipher text is properly transformed from the original IBE cipher text, if the authorization token used in the transformation was created by the user who is capable of decrypting the original cipher text. Also, the second condition defines that a transformed cipher texts can be decrypted by the data consumers whose identities are indicated in the authorization token.

B. *Formal Security Definitions*

We present formal security definitions to capture the *indistinguishability of cipher texts against selective identity and chosen-plaintext attack* (IND-SID-CPA) launched by unauthorized clients and curious CSP, and the *leakage-resistance of private keys against collusion attack* (LR-CA) launched by authorized clients and CSP. For the former, we prevent an adversary, which is not given a valid private key for decryption,from gaining access to the data encrypted in IBE or IBBE cipher text. For the latter, we prevent an adversary, which couldcollude with authorized clients and CSP by having their privatekeys and authorization tokens, respectively, from recovering the private keys that were used to generate the authorization tokens. We note that if the private key of a data owner is compromised, then all the owner's data stored in CSP are revealed to the adversary.

First consider the case where unauthorized clients or malicious CSP try to access the data encrypted in IBE cipher text or transformed (IBBE) cipher text. Let A bea probabilistic polynomial-time adversary, which plays the following game with the challenger C and tries to distinguish two encrypted messages.

Setup: The adversary A chooses a target identity ID^* and sends it to the challenger. With security parameter λ and the maximum number m of authorized data consumers, the challenger C runs the Setup algorithm to generate system public parameters PP and master secret keys MSK. It gives PP to A and keeps MSK secret.

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Guess: The adversary A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

The advantage of A in this game is defined as

Definition 1: An IBET system is IND-SID-CPA secure if all probabilistic polynomial-time adversaries have at most a negligible advantage in the above game.

In the challenge phase of the above game, the two restrictions are to prevent the adversary A from winning the game ina trivial way. Specifically, if the adversary has a private key for ID^*, then it can correctly decrypt the challenge cipher text

CT_{ID^*} and always output $b' = b$. If the adversary has a private key for $ID_i \in S_i$ and an authorization token for ID^* and S_i, it can first convert CT_{ID^*} into CT_{S_i} and then use the private key of ID_i to decrypt CT_{S_i}. In this way, the adversary can also always output $b' = b$.

We note that Definition 1 covers the security against unauthorized access attack to the data stored in both IBE andI BBE cipher text formats. The adversary, which is challenged with an IBE cipher text CT_{ID^*}, can query authorization token $TK_{ID^* \to S}$ and then apply $TK_{ID^* \to S}$ to transform CT_{ID^*} into a transformed IBBE cipher text CT_S. This means that in the IBET system, unauthorized clients and CSP have accessto both IBE and IBBE cipher texts. Definition 1 says that a secure IBET scheme can resist unauthorized access to the dataencrypted in any cipher text.

AN IBET SCHEME

TABLE I NOTATIONS

It is challenging to achieve the mechanism that transformsa file allowing just one authorized visitor, into another file thatallows multiple ones. At first sight, it seems that the original authorized visitor could employ IBBE to encrypt his private key for all the intended receivers, so that each one of them can obtain the private key and then decrypt the file just asthe authorized visitor does. This, however, exposure of the authorized visitor's private key would lead to an unwanted access to outsourced data.

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

To achieve the encryption transformation while maintainingthe secrecy of private keys, we introduce a *privacy-preserving authorization* method to the construction of IBET. Specifically,when generating an authorization token, the data owner blinds his private key by a random factor; CSP uses the authorizationtoken to transform a file and obtains a transformed file that is the result of the plaintext blinded by the random factor. Only the authorized data consumers can obtain the random factor from the transformed file and then recover the plaintext. In thisway, the data owner's private key is well protected.

From a technical point of view, we follow Boneh and Boyen's identity-based encryption scheme [31] in our construction but compress the public parameters by reducing one element. We also employ Delerablée's identity-based broadcast encryption scheme [9] to achieve the multi-receiver functionality. The authorization token is generated by applyingonce the IBBE encryption and the transformed file is in Delerablée's IBBE-type cipher text format.

A. *Construction*

In this section, we present our IBET construction built on bilinear groups. Table I summarizes the notations throughout the paper.

Suppose G and G_T are two (multiplicative) cyclic groups ofprime order p. A bilinear map $e(\cdot, \cdot)$ is a map G G G_T which has the following properties: 1) *Bilinearity*: for all g, h G and all a, b Z_p, $e(g^a, h^b)$ $e(g^b, h^a)$ $e(g, h)^{ab}$; 2) *Non-degeneracy*: $e(g, h)$ 1. We say that G isa bilinear group if the group operations in G and the bilinearmap $e : G \times G \rightarrow G_T$ can be efficiently computed.

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Symbol	Meaning
$\mathbb{G}, \mathbb{G}_T$	Cyclic groups with bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
p	The large prime order of groups $\mathbb{G}$ and $\mathbb{G}_T$
g	A generator of $\mathbb{G}$
PP	The system public parameters
MSK	The system master secret key
H_0, H_1	Two cryptographic hash functions
ID	An identity of a user, e.g., an email address
S	A set of different identities, i.e., $S = \{ID_i\}$
SK_{ID}	A private key for the user with identity ID
CT_{ID}	An IBE ciphertext in an original file
CT_S	An IBBE ciphertext in a transformed file
s, t, r	Random values in $\mathbb{Z}_p^*$
u, h	Random values in $\mathbb{G}$
	the maximum number of data consumers
	who can access the same data
n	the number of data consumers specified by a data owner

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

$(g, g^x, g^{x^2}, \ldots, g^{x^q})$ G^{q+1} and a *fixed* value c Z_p, the probability of any PPT algorithm A in computing $g^{1/(x+c)}$ is negligible. We note that the value c is fixed in this version

of q-SDH assumption, while, by contrast, it is freely chosen in the standard q-SDH assumption [32]. Boneh *et al.* has already discussed this variation of q-SDH assumption in [33], but for completeness we still give a proof (in Appendix A) that this variation of q-SDH assumption holds in any group where the q-SDH assumption holds.

1) System Setup: The trusted party RA generates two cyclic groups G and G_T of prime order $p > 3$ and a bilinear map $e : G \times G \rightarrow G_T$. RA chooses a random generator $g \in G$

and random values $\alpha \in Z_p^*$ and $h, u \in G$. Then it computes

$g_1 g^{\alpha}$ and $u^{\alpha}, h^{\alpha}, h^{\alpha^2}, \ldots, h^{\alpha^m}$ G, where m is set as the maximum size of the set of data consumers who can access the same data. RA also selects two cryptographic hash functions $H_0 : \{0,1\}^* \rightarrow Z_p^*$ and H_1 G_T $\rightarrow$ G. The hash function H_0 can be implemented by applying standard hash functions such

as SHA-2 and the hash function H_1 can be realized by using the Map To Point encoding function [6]. Specifically, given the underlying elliptic curve (e.g., $y^2 = x^3 + 1$ over F_q, where

$q = 4p - 1$ and p does not divide 4) of G, for an input

Our IBET scheme will rely on the following complexity

assumptions.

General Decisional Diffie-Hellman Exponent (GDDHE) assumption [9]. Suppose G is a cyclic group of prime

$X \in G_T$, first use a hash function $G : \{0, 1\}^* \rightarrow F_q$ to map X to an element $y_0 \in F_q$ and then compute $x_0 \in F_q$ such that $Q = (x_0, y_0)$ is a point on the elliptic curve. Then take

order p and $g_0, h_0 \in$ G. Let P and Q be two co prime polynomials with pair wise distinct roots, of respective orders q and k. The GDDHE assumption says

that given $(g_0, g^{\alpha}, \ldots, g^{\alpha^{q-1}}, g^{\alpha P(\alpha)}, g^{s\alpha P(\alpha)}) \in G^{q+2}$,

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Y Q^4 G of order p as the output of $H_1(X)$. More details about Map To Point can be found in [6]. The system publicparameters and master secret key are defined as

Third International Conference on "Materials, Computing and Communication Technologies"
in association with International Journal of Scientific Research in Science,
Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

α $(h_0, h_0, \ldots, h_0^{\alpha^{2k}}, h_0) \in G^+$ and $T \in G_T$, the

$PP = g, u, u^{\alpha}, h, h^{\alpha}, h^{\alpha^2}, \cdots, h^{\alpha^m}, e(g,h), H(\cdot), H(\cdot)$

ability of any probabilistic polynomial-time (PPT) algorithmin deciding whether T is equal to $e(g_0, h_0)^{sP(\alpha)}$ or is A a $=$

random value of G_T is negligible.

A variation of q-SDH assumption [32]. We give a natural variation of the q-Strong-Diffie-Hellman (q-SDH) assumption. Suppose G is a cyclic group of prime order p. The variationof q-SDH assumption states that, given a tuple of elements and MSK (g, α).

User Registration: In this procedure, a user asks RA for joining in the system. RA first checks the validation ofthe requestor. If the user passes, RA generates an authorized credential (e.g., a private key). Suppose that the requesting user is associated with an identity ID. RA uses its master secret key and the hash function H_0 to compute Then RA gives SK_{ID} to the user through a secure channel.

2) *File Creation:* When using the storage service provided by CSP to store data, the data owners encrypt their data and outsource the resulting files to CSP. The files are stored in cipher text format and can only be accessed by authorized data consumers. In practice, *key encapsulation* is a typical technique to reduce the costs of encryption. In such technique,a data owner first encrypts his data via a symmetric encryptionmechanism (e.g., AES) and then encrypts the symmetric encryption key with the asymmetric encryption. The performance of the asymmetric encryption is thus independent of the data size. Our IBET scheme also follows this technique.A data owner first picks a random symmetric key M G_T and uses it to encrypt the data to be outsourced to CSP. Then the data owner employs IBE encryption mechanism to encrypt M. According to different data sharing requirements, there are two cases where data owners encrypt M.

Case 1: Some data should be accessed by only one user. For example, a mobile user encrypts his private photos to be stored in clouds and wants just himself to be able to access. In such case, the user (data owner) chooses a

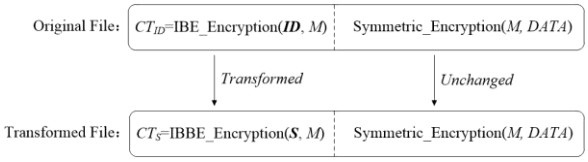


Fig. 3. File transformation.

where SK_{ID} is the private key of the data owner. The authorization token is set as $TK_{ID \to S} = (d_1, d_2, d_3, d_4)$. Then the data owner sends $TK_{ID \to S}$ to CSP.

5) File Transformation: Receiving the data owner's authorization token, CSP starts to transform the specified file. In fact, CSP just needs to transform the IBE cipher text (precisely, case 2 cipher text) about the symmetric key of the file. The other part of the file, i.e., encryption of data underthe symmetric key, remains unchanged (see Fig. 3). Given the

authorization token $TK_{ID \to S} = (d_1, d_2, d_3, d_4)$ and the IBE cipher text $CT_{ID} = (C_0, C_1, C_2)$, CSP transforms CT_{ID} to be $CT_S = (c_1, c_2, c_3, c_4, c_5)$ where $c_1 = d_1, c_2 = d_2, c_3 = d_3, c_4 = C_2$ and

$c_5 = C_0 / e(C_1, d_4)$

$= M \cdot e(g,h) / e \quad h \quad ,$

$s(\alpha + H(ID)) \qquad -\alpha + H(ID)$

random value $s \in Z_p^*$ and computes

$C_0 = M \cdot e(g,h)^s, \quad C_1 = h^{s(\alpha + H0(ID))}.$

$h^{s(\alpha + H0(ID))}, u^r \quad .$

Then $CT_{ID} \quad (C_0, C_1)$ is the cipher text for M, where
ID is the identity of the intended data consumer.

· *Case 2:* Some data would be shared with multiple users but the identities of these users cannot be determined beforehand. For instance, a patient feels that his health records may be diagnosed by different doctors, but for now, he can just determine one doctor. In this case,
the patient (data owner) chooses a random value $s \in Z_p^*$

and computes

$C_0 = M \cdot e(g,h)^s, \quad C_1 = h^{s(\alpha + H0(ID))}, \quad C_2 = u^{s(\alpha + H0(ID))}.$

Then $CT_{ID} = (C_0, C_1, C_2)$ is the cipher text for M.
The cipher text of case 2 includes one more component than that of case 1. This component is crucial for transformation. Thus, only the files created in case 2 can be transformed.

Finally, CT_{ID} and the encryption of data under M form the file outsourced to CSP.

4) Authorization: When a data owner (or an authorized dataconsumer) finds that additional users should be authorized to

This transformed cipher text $C\ T_S$ is an IBBE-type cipher text. Then, cipher text $C\ T_S$ and the (unchanged) encryption of data form a transformed file in CSP.

6) File Access: There are two kinds of files in the system, i.e., the original files and the transformed files. The access about these two kinds of files are described as follows.

· *Original files:* An original file contains an IBE cipher textof a symmetric key. For an IBE cipher text $CT_{ID}\ (C_0, C_1)$ (case 1 cipher text) or $CT_{ID}\ (C_0, C_1, C_2)$(case 2 cipher text) that is associated with identity ID, the data consumer with the same identity ID uses $C_0$and C_1 to compute: $M = C_0/e(SK_{ID}, C_1)$. Then the data owner uses the symmetric key M to finally recoverthe data.

· *Transformed files:* A transformed file contain an IBBE cipher text that is converted from an original IBE cipher- text. For an IBBE cipher text $C\ T_S\ (c_1, c_2, c_3, c_4, c_5)$ associated with the identity set S, a data consumer with identity $ID_i \in S$ can compute

[1]. , and W. Shi, “Asymmetric cross-cryptosystem re-encryption applicable.

[2]. J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, “Anonymous identity based broadcast encryption with revocation for file sharing,” in Proc. Australia’s. Conf. Inf. Secur. Privacy. Cham, Switzerland: Springer, 2016, pp. 223–239.

[3]. J. Lai, Y. Mu, F. Guo, and R. Chen, “Fully privacy-preserving ID-based broadcast encryption with authorization,” Comput. J., vol. 60, no. 12, pp. 1809–1821, Dec. 2017.

[4]. W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y.-W. Chow, “Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext,” in Proc. 11th ACM Asia Conf. Comput. Commun. Secur. ASIA CCS, 2016, pp. 201–210.

[5]. J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, “Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city,” Pers. Ubiquitous Comput., vol. 21, no. 5, pp. 855–868, Oct. 2017.

[6]. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Advances in Cryptology—EUROCRYPT. Berlin, Germany: Springe, 1998, pp. 127–144.

[7]. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Trans. Inf. Syst. Secur. (TISSEC), vol. 9, no. 1, pp. 1–30, Feb. 2006.

[8]. Libert and D. Vergnaud, “Unidirectional chosen-cipher text secure proxy re-encryption,” in Public Key Cryptography—PKC. Berlin, Germany: Springer, 2008, pp. 360–379.