# Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud

**Dr.N.Satheesh[1], Dr.M.Narayanan[2], Dr.G.Jawaharlel Nehru[3], Ms. Zaheeda Parveen[4]**
[1,3]Associate Professor, Department of CSE, St. Martin’s Engineering College, Secunderabad, Telangana
[2]Professor & HOD, Department of CSE, St. Martin’s Engineering College, Secunderabad, Telangana.
[4]Assistant Professor Department of CSE, St. Martin’s Engineering College, Secunderabad, Telangana.

Abstract—with the quick improvement of appropriate taking care of a growing number of individuals and affiliations are sharing data in the public cloud. To get the attestation of enlightening records to the side in the cloud, a data owner by and large scrambles data with the genuine that particular entrusted data customers can disentangle the data. This raises an essential issue when the mixed data ought to be shared with more people past those at first allotted by the data owner. To choose this issue, we introduce and formalize an individual-based encryption change (IBET) model through immaculately combining two grounded encryption parts, to be express individual-based encryption (IBE) and character-based transmission encryption (IBBE). In IBET, data customers are seen and upheld for data access subject to their prominent characters, which sidesteps baffled exposure to the board in conventional secure passed-on structures. Significantly more on a very basic level, IBET gives a change framework that change over an IBE ciphertext into an IBBE ciphertext so one more assembling of customers not shown during the IBE encryption can get to the limited data. We plan a basic IBET plot reliant upon bilinear get-togethers and show its insurance from stunning attacks. Cautious speculative and test appraisals show the high capacity and practicability of the proposed plot.

## 1. INTRODUCTION

Cloud computing provides powerful and flexible storage services for individuals and organizations [1] brings about lots of benefits of sharing data with geographically dispersed data users, and significantly reduces local burden of storage management and maintenance. However, the concerns on data security and privacy are becoming one of the major obstacles impeding more widespread usage of cloud storage [2], since data owners lose physical control on their data after data are outsourced to cloud servers maintained by a cloud services provider (CSP). Data owners may worry about whether their sensitive data have been accessed by unauthorized users or malicious CSP.

Cryptographic encryptions are widely suggested as standard approaches to protect the security and privacy of data outsourced to clouds [3]. With encryption mechanisms, dataowner’s first encrypt their data and then outsource to cloud servers. Then the data in clouds are stored in ciphertext format and can only be accessed by the users having matching decryption keys. In a public cloud storage system, where different data owners may employ different encryption mechanisms according to their own data sharing requirements, it is often that a data owner wants to share his data with only one user and thus encrypts the data to generate a particular ciphertext that can only be decrypted by the specific user. However, as data sharing requirement changes, the same data owner would like to share his data with more users, which, therefore, requires to transform the ciphertext format so that multiple users can decrypt.

There are many scenarios in which the ciphertext trans-formation mentioned above is highly desirable. Consider a group of medical insurance agents draft a health insurance plan for a client. To do so, each agent needs to collect the client’s personal information (e.g., electronic health records, occupations data, and financial reports) from various data sources such as hospitals, employers, tax departments. The required data may be stored in remote cloud servers and especially, may be encrypted under different encryption mechanisms. To allow the agents to read and make use of the required data, a naive way is to let each agent acquire the corresponding decryption keys from the authorities who manage respective data. However, this would pose great concerns on data privacy. The authorities would ask a natural question: “If I give my decryption key to the agents, how to assure that all the agents would not leak the decryption key or use the decryption key to access other clients’ stored data?”

This paper attempts to solve such problem technically so that the authorities can transform the ciphertexts from oneencryption system to another, without handing over their decryption keys. In particular, we consider an encryption transformation mechanism that connects two types of well-established encryption systems, i.e., identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). We take electronic health records sharing as a motivation of our work.

Suppose a patient is equipped with implantable or wearable medical sensors to collect personal physiological records. These records are aggregated at a mobile device and then uploaded to a remote server. To protect personal privacy, the patient may encrypt his health records by some encryption mechanism, e.g., IBE, so that only his doctor can read the health records and then make proper diagnosis. At some point, the doctor finds a complicated situation about the patient’s health and consequently, decides to consult a group of experts from different hospitals. For full understanding of the patient’s health condition, the experts first need to read the health records (see Fig. 1). Since the records are encrypted previously, the experts are impossible to directly read the data. Meanwhile, the encryption method taken by the patient and the corresponding decryption key are unknown to the experts. This result in a dilemma for the experts: “How could we read the patient’s health records in order to provide our treatment advices?”

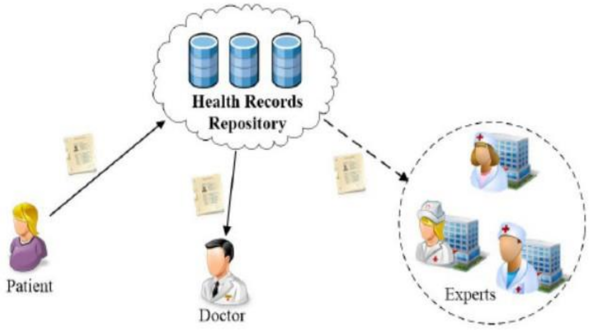


**Fig.1 Electronic Health Records Sharing with More Doctors**

A trivial solution would be that the doctor first decrypts all the encrypted records and then sends out the data in plaintext format to each expert. This, however, may be impractical for the doctor since a considerable computation and communication costs may be caused due to the massive health data uploaded every day. More importantly, there is a risk of privacy disclosure by sending data in plaintext format.

There exists a cryptographic tool called Proxy Re-Encryption (PRE) that would be of help here. PRE can transform the doctor’s plaintext information into a ciphertext that can be decrypted by one expert. Then, for n experts, PRE needs to run n times repeatedly for transferring the patient’s health data to all experts, which is inefficient. We observe that IBBE achieves a useful encryption mechanism that allows multiple users to simultaneously decrypt a ciphertext. Thus, we ask: “Can we find an efficient way to transform the encrypted data in IBE ciphertext format into an IBBE ciphertext so that multiple users can decrypt at the same time?”

## Our contributions

In this paper, we try to answer the above question by studying encryption transformation between two different encryption systems. For the first time, we propose a novel notion called identity-based encryption transformation (IBET). We also define the notion (including algorithm definition and security model) of IBET. Then we design a concrete IBET scheme in bilinear groups, which provides the following attractive 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 in the server in IBE/IBBE ciphertext 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 and IBBE. In particular, a data owner (or an authorized data consumer) can transform the data stored in IBE ciphertext format into the data in IBBE ciphertext format, so that a set of user’s specified by the data owner (or the authorized data consumer) can simultaneously access the data.
- **Strong security guarantee:** Our IBET scheme achieves a strong 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.

We also conduct a series of experiments on our IBET scheme and make comparisons with some related schemes. The result of the IBET mechanism gets high performance in transforming the encrypted data, without incurring any significant computation costs to cloud clients or cloud servers.

Applications: the IBET mechanism can be applied to many data-sharing applications. First of all, the example of health records sharing described previously is an appropriate area where our IBET can be applied. Cloud-based encrypted email forwarding is another possible application. Imagine that several companies deploy their email systems on cloud servers. The IBET mechanism can be used to transform an encrypted email destined for an employee in one company into an encrypted email that can be received and decrypted by multiple employees in different companies. A vehicular ad-hoc network is also a potential application for IBET. When a car receives an encrypted report about the front car condition or accident ahead and would like further to broadcast the situation to rear vehicles, IBET can be used to directly transform the encrypted report into a broadcast ciphertext that allows multiple receivers to decrypt. Last but not least, in a mobile office environment, IBET may be utilized as a mobile application to securely share business information with a company director via a public cloud, and then transform the encrypted business data (if requested) so that the whole management team can access it

**Proposed System**

- Per attempts to manage such issues believe it or not so the specialists can change the code texts.
- More out and out, IBET gives a change instrument that changes over an IBE figure text into an IBBE figure text so another gathering of not actually settled forever during the IBE encryption can get to the privileged information.
- We plan a liberal IBET plot dependent upon bilinear get-togethers and show its protection from astonishing assaults. Careful hypothetical and exploratory appraisals show the high capacity and practicability of the proposed conspire

**Advantages**

- Providing information-driven confirmation.
- Its confirmation from staggering assaults.
- High capacity and practicability of the proposed conspire.

**Paper Organization**

The rest of the paper is organized as follows. We describe theIBET system architecture, threat model and security goals in Section 2. The framework and security definition of the IBET system are formalized in Section 3. We present a concrete IBET scheme in Section 4. The security and results in Section 5 and Finally, Section 6 concludes the paper.

## II. RELATED WORKS

Outsourced data protection. Cryptographic Encryption methods have been extensively used to secure information outsourced to clouds. Traditional public key encryption techniques are applied to get user centric access control on outsourced data [4], [5]. Identity-based encryption (IBE) [6]technique is a promising encryption tool which eliminates trusted certificates for all users.

Wei et al. [7] exploited IBE to secure information sharing in mobile computing environments. He et al. [8] employed IBE transformation method to construct a three-way handshake method in healthcare social network to secure information exchanged between patients.

The IBBE[9] transformation method extends IBE to support multi-user encryption in the sense that a user encrypts a message once for multiple intended receivers. In-light of that useful feature, Deng et al. [10] utilized IBBE method in cloud storage systems to allow multiple authorized usres to access the same outsourced file. To invoke some users from the initial receiver set of the IBBE transformation method, a number of revocable IBBE schemes are proposed [11], [12], [13], [14].

Inter-domain Transformation. Blaze et al. [15] first introduced the concept of proxy re-encryption to handle ciphertext transformation within an encryption system. With this PRE, a user can transform a ciphertext generated under Alice’s public key into a ciphertext 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 privacy of PRE and most of them focus on unidirectional PRE. LibertandVergnaud [17] presented the first unidirectional PRE scheme. Cao et al. [18] implemented the autonomous path PRE technique to enable a user to designate a path of preferred authorized users to his outsourced information. Guo et al. [19] introduced accountability into unidirectional PRE method to identify the proxy which abuses its re-encryption keys.

By combining PRE and IBE techniques, Green and Ateniese [20]implemented the identity-based PRE (IBPRE) mechanism, which is an extension of PRE in identity-based settings. Chu and Tzeng[21] implemented an IBPRE mechanism with short ciphertext 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 authenticate information about data owners. Liang et al. [22] overcome this security issue by implementing the cloud-based revocable IBPRE mechanism. This mechanism requires the intereface between data owners and a secret key generator authority for each transformation, which may result an efficiency problem. Xu et al. [23] implemented an IBBE-based PRE techniques by introducing IBBE into PRE techniques.Apart from IBPRE, 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 ciphertext transformation in the same encryption system, that is, ciphertexts cannot be converted into another format.

Cross-domain transformation. There are a few schemes achieving cross-domain encryption transformation. Matsuo[28] linked the traditional public-key encryption and identity-based encryption by allowing to transform aciphertextof public key systems into a ciphertext of IBE systems.. Mizuno and Doi [29] also implemented a unidirectional PRE method that transforms ciphertexts of an attribute based encryption into ciphertexts of an IBE system, while requiring users to interact with each other and store additional information for transformation. Recently, Jianget al. [30] implemented a cross-domain encryption switching scheme that connects traditional public-key encryption and identity-based encryption, while it requires cryptographic certificates for all the users in the public-key encryption system. This paper aims at addressing cross-domain transformation in identity-based settings; thus saves the cost for certificate management. Moreover, this paper provides encryption transformation from (one-receiver) IBE system to (multi-receiver) IBBE system so that one's data can be shared with more users even though the information have already been encrypted.

## 3. SYSTEM MODEL

### System Architecture

The architecture of IBET system is shown in Fig. 2. An IBET method consists of four types of entities, that is, data owners, data consumers, registry authority (RA) and cloud service provider (CSP). Generally, data owners and data consumers are both cloud clients. RA is a trusted party that is responsible for setting up system, responding to registration requests and issuing public parameters for file outsourcing. CSP has two 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. In this way, all the (registered) employees can make use of storage and computation services.

Data owners can outsource data to CSP. Specifically, to protect information, data owners can employ IBE encryption transformation technique to process data and then outsource the resulting files (data in ciphertext format) to CSP. Suppose that a file is the result of IBE encryption method for some data (thus the data can be accessed by only one data consumer). If the corresponding data owner further wants to share the data with more data consumers, he generates an authorization token and sends it to CSP; then CSP can translate the file in IBE ciphertext format into a file in IBBE ciphertext format so that all designated data consumers can decrypt and then access the data. In this way, for the data previously encrypted by IBE and originally accessible to only one data consumer, the data owner can authorize more data consumers to access it.

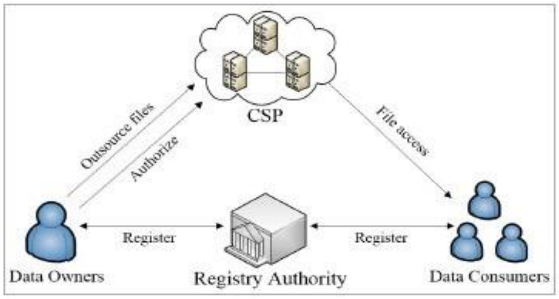


**Fig.2System Architecture**

### Threat Model and Security Goals

2.2 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 of authorization. Considering these realistic attacks, we require that a secure IBET system should at least satisfy the following security goals.

- **Data security protection:** If data have been encrypted before outsourced, then only the clients holding correct decryption keys can access (theseclient 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.

## 4. METHODOLOGY

- **Data Owner:**

The proprietor of the information utilizes appropriated limit relationship to store the records. Before information re-appropriating, the proprietor of the information disposes of the arrangement of watchwords from the record and encodes in a reliable archive. The report is besides blended to Encrypted message During the encryption cycle, the passage really not yet decided and acquainted in the cipher text with perform fine-grained consent control. There will be 3 information proprietors in our undertaking, a public key and a clandestine key will be made at the hour of moving the report.

- **Registry Authority (RA)**

RA can make as far as possible for the construction and the game plans of public/secret keys for clients. Right when the client's mystery the key is spilled for advantage or different purposes, RA runs a way assessment to track down the malevolent client. After the cheat is Tracked, RA will deny cloud server client

- **Data Consumer:**

very information client has a tremendous heap of characteristics to depict their qualities. The blueprint of qualities is inserted in the client's dark key. By utilizing the odd key, the information client can look through the encoded reports put away in the cloud, that is, pick an immense heap of clarifications to look. If the approach of client credits full fills the section strategy depicted in the encoded records, the cloud server reacts to the client's advantage deals and tracks down the sorting everything out with archives. In any case, the pursuit demand is exonerated. Right when the coordinating with records arereturned, the client executes the making a comprehension of calculation to recover the plain text.

- **Cloud Service Provider (CSP)**

In this last module of our endeavor after useful cloud stage login endeavor supervisor will be diverted to his page where he will notice the choices like All User Details, All Request Details and All Files Details On tapping on every hyperlink he will truly have to perceive what activities cloud clients are doing in the cloud. CSP reasonably has 'huge' information extra room. Stores and controls encoded information rethought from the selected gatherings in the arrangement. In like manner, CSP gives assessment ability to perform homomorphic practices over blended information.

- **Traitor Tracing**:

This is the last module of our undertaking where our proposed system happens, in this module attacker will send the courses of action for open records to some optional individuals present in the affiliation, if any client reacts to the referring to sent by the aggressor and sends the key, he will be followed and revocated from the cloud server

## 5. PROPOSED ALGORITHM

Identity-Based Encryption Transformation (IBET)
Plan of IBET System Formally, an IBET structure incorporate six polynomial-time quantifiable estimations, that is, Setup, Register, Encrypt, Authorize, Transform, and Decrypt.

- **Setup(1$\lambda$,m) → (PP,MSK) :** The development plan estimation, run by RA, takes as data a security limit $\lambda$ and the allowed maximal number m of data clients embraced to get to comparable data. It yields quite far PP for the plan and the master secret key MSK for RA itself.
- **Register(PP,MSK, ID) → SKID :** The selection computation, run by RA, takes as data quite far PP, the master secret key MSK and an individual ID $\in \{0, 1\}*$. It yields a private key SKID.
- **Encrypt(PP,M, ID) → CTID :** The encryption estimation, run by a data owner, takes as data beyond what many would consider possible PP, the message M to be mixed and an individual ID. It yields an IBE ciphertext CTID.
- **Authorize(PP, SKID, S) → TKID→S:** The guaranteeing computation, run by a data owner with character ID, takes as data the data owner's private key SKID, beyond what many would consider possible PP and the set S of characters of data clients. It yields a help token TKID→S.
- **Transform(PP, TKID→S,CTID) → CTS:** The change estimation, run by CSP, takes as data the help token TKID→S, quite far PP and the IBE ciphertext CTID. It yields a changed (IBBE) ciphertext CTS.
- **Decrypt(PP,CTID/CTS, SKID′ ) → M/$\perp$**: The unscrambling computation, run by a data purchaser ID′, takes as information quite far PP, a private key SKID′ and a ciphertext CTID or CTS. For CTID, it yields the message M if ID = ID′ and a phony picture $\perp$ regardless; for CTS, it yields the message M if ID′ $\in$ S and a fake picture $\perp$ in any case.

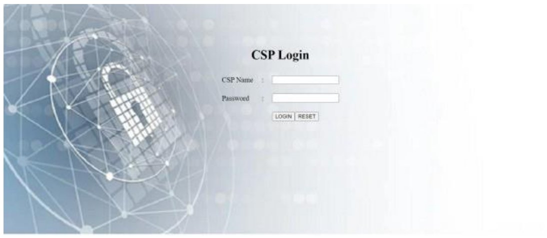
A secure IBET scheme should be sound, that is, if each entity honestly follows the scheme, then any failure wouldnot happen during the scheme running. Formally, for any(PP,MSK) ← **Setup**(1$\lambda$,m), the following conditions must be satisfied:

- For any IBE ciphertext CTID ← **Encrypt**(PP,M, ID ) and any private key SKID′ ← **Register**(PP, ID′, MSK), if ID = ID′, then the decryption algorithm **Decrypt**(PP,CTID, SKID′ ) always outputs the plaintext M.
- For any transformed ciphertext CTS ← **Transform**(PP, TKID→S,CTID), where TKID→S ← Authorize (PP, SKID, S) and CTID ← **Encrypt**(PP,M, ID), and any private key SKID′ ← **Register**(PP,MSK, ID′), if ID′ $\in$ S, the decryption algorithm **Decrypt**(PP,CTS, SKID′ ) always outputs the plaintext M.

The first condition is straightforward. It means that any encrypted message in IBE ciphertext 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 ciphertext (from an IBE ciphertext) can be correctly decrypted by all intended data consumers. Thus, we must define what is a properly transformed ci-phertext and who are the intended data consumers able to decrypt the ciphertext.

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

## 6. RESULT

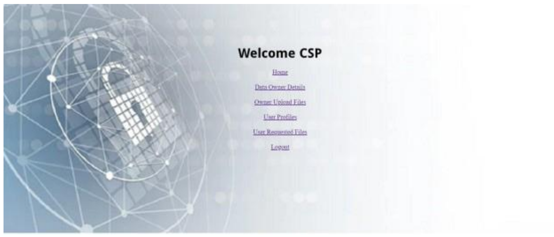


CSP Login

CSP Name :

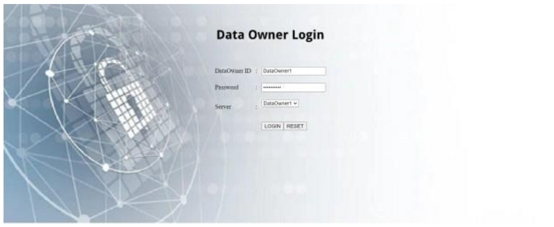
Password :

Fig.3CSP Login Page



Welcome CSP

Fig.4CSP Details



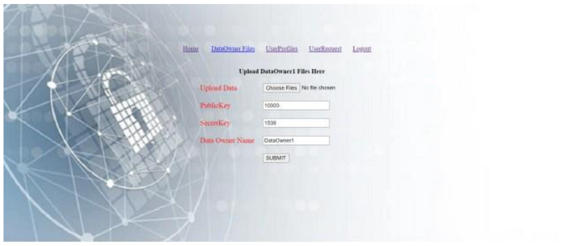
Data Owner Login

DataOwner ID : DataOwner1

Password : ••••••••••

Server : DataOwner1

Fig.5Owner Login Page



Upload DataOwner1 Files Here

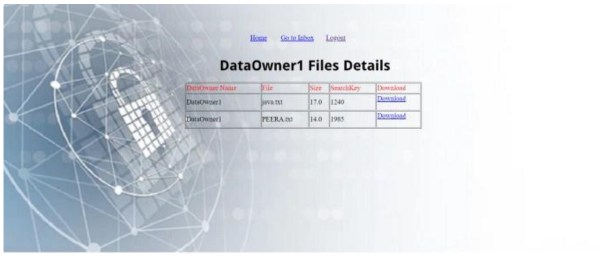
Upload Data: Choose Files No file chosen

PublicKey: 10000

SecretKey: 1539

Data Owner Name: DataOwner1

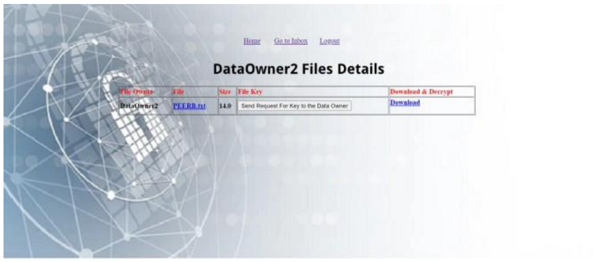
Fig.6File Upload Details



DataOwner1 Files Details

| DataOwner Name | File | Size | SearchKey | Download |
|---|---|---|---|---|
| DataOwner1 | java.txt | 17.0 | 1240 | Download |
| DataOwner1 | PEERA.txt | 14.0 | 1985 | Download |

Fig.7 Owner Files Details



DataOwner2 Files Details

| File Owner | File | Size | File Key | Download & Decrypt |
|---|---|---|---|---|
| DataOwner2 | PEERB.txt | 14.0 | Send Request For Key to the Data Owner | Download |

Fig.8Security Files

## 7. CONCLUSION AND FUTURE WORK

n this paper we studied how to securely and efficiently transform encrypted data in clouds. To address this issue, we proposed an identity-based encryption transformation (IBET) model, which connects the well-studied IBE and IBBE systems. IBET allows data owners to secure outsourced data with identity-based access control, which eliminates complicated cryptographic certificates for all users. Moreover, IBET provides a transformation mechanism for data owners to authorize cloud service provider (CSP) to transform a file in IBE-ciphertext formant into a file in IBBE-ciphertext format, so that a set of authorized users can access the underlying data. We proposed a concrete IBET scheme that is secure against powerful attacks. Thorough experimental analyses demonstrate the efficiency and practicability of the scheme.

## REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection for the masses,” Computer, vol. 45, no. 1, pp. 39–45, 2012.

[2] J. Yu, K. Ren, and C. Wang, “Enabling cloud storage auditing with verifiable outsourcing of key updates,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375,2016.

[3] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, “Achieving secure, universal, and fine-grained query results verification for secure search scheme over

encrypted cloud data," IEEE Transactions onCloud Computing, 2017.

[4] K. Li, W. Zhang, C. Yang, and N. Yu, "Security analysis on one-tomanyorder preserving encryption-based cloud data search," IEEETransactions on Information Forensics and Security, vol. 10, no. 9, pp.1918–1926, 2015.

[5] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: a survey," IEEE Transactions on Services Computing, Vol. 11, no. 6, pp. 978–996, 2018.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[7] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEETransactions on Cloud Computing, 2016.

[8] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, andA. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network,"IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4,pp. 633–645, 2018.

[9] C. Delegable, "Identity-based broadcast encryption with constant sizeciphertexts and private keys," in International Conference onthe Theory and Application of Cryptology and Information Security.Springer, 2007, pp. 200–215.

[10] H. Deng, Q.Wu, B. Qin,W. Susilo, J. Liu, andW. Shi, "Asymmetric Ross-cryptosystem-encryption applicable to efficient and secure mobile access to outsourced data," in Proceedings of the 10th ACMSymposium on Information, Computer and Communications Security.ACM, 2015, pp. 393–404.

[11] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing,"in Australasian Conference on Information Security and Privacy. Springer, 2016, pp. 223–239.

[12] J. Lai, Y. Mu, F. Guo, and R. Chen, "Fully privacy-preserving-based broadcast encryption with authorization," The ComputerJournal, vol. 60, no. 12, pp. 1809–1821, 2017.

[13] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y.-W. Chow,"Recipient revocable identity-based broadcast encryption: howto revoke some recipients in ibbe without knowledge of theplaintext," in Proceedings of the 11th ACM on Asia Conference onComputer and Communications Security. ACM, 2016, pp. 201–210.

[14] 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," Personal and Ubiquitous Computing, Vol. 21, no. 5, pp. 855–868, 2017.

[15] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in EUROCRYPT 1998. Springer Berlin Heidelberg, 1998, pp. 127–144.

[16] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," Information and System Security (TISSEC), ACMTransactions on, vol. 9, no. 1, pp. 1–30, 2006.

[17] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertextsecure proxy re-encryption," in PKC 2008. Springer Berlin Heidelberg,2008, pp. 360–379.

[18] Z. Cao, H. Wang, and Y. Zhao, "Ap-pre: Autonomous path proxyre-encryption and its application," IEEE Transactions on Dependable and Secure Computing, 2017.

[19] H. Guo, Z. Zhang, J. Xu, N. An, and X. Lan, "Accountable proxy re-encryption for secure data sharing," IEEE Transactions on Dependable and Secure Computing, 2018.

[20] M. Green and G. Ateniese, "Identity-based proxy re-encryption,"in ACNS 2007. Springer Berlin Heidelberg, 2007, pp. 288–306

[21] C. K. Chu and W. G. Tzeng, "Identity-based proxy re-encryption without random oracles," in ISC 2007. Springer Berlin Heidelberg,2007, pp. 189–202.13

[22] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in European Symposium on Research in Computer Security. Springer, 2014, pp. 257–272.

[23] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identitybasedbroadcast proxy re-encryption and its application to cloudemail," IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79,2016.

[24] K. Liang, M. H. Au, J. K. Liu,W. Susilo, D. S.Wong, G. Yang, Y. Yu,and A. Yang, "A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95–108, 2015.

[25] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for drop box data sharing system," Designs,Codes and Cryptography, pp. 1–17, 2018.

[26] Y. Yang andM.Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for ehealthclouds," IEEE Transactions Information Forensics and Security, Vol. 11, no. 4, pp. 746–759, 2016.

[27] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang,T. V. X. Phuong, and Q. Xie, "A dfa-based functional proxy re-encryptionscheme for secure public cloud data sharing," IEEETransactions on Information Forensics and Security, vol. 9, no. 10, pp.1667–1680, 2014.

[28] T. Matsuo, “Proxy re-encryption systems for identity-based encryption,”in Pairing 2007. Springer Berlin Heidelberg, 2007, pp.247–267.
[29] T. Mizuno and H. Doi, “Hybrid proxy re-encryption scheme forattribute-based encryption,” in International Conference on Information Security and Cryptology. Springer, 2009, pp. 288–302.
[30] P. Jiang, J. Ning, K. Liang, C. Dong, J. Chen, and Z. Cao, “Encryption switching service: Securely switch your encrypted datato another format,” IEEE Transactions Services Computing, 2018.
[31] D. Boneh and X. Boyen, “Efficient selective-id secure identity-based encryption without random oracles,” in EUROCRYPT 2004.Springer Berlin Heidelberg, 2004, pp. 223–238.
[32] “Short signatures without random oracles and the sdh assumption in bilinear groups,” Journal of Cryptology, vol. 21, no. 2, pp. 149–177, 2008.
[33] D. Boneh, X. Boyen, and E. J. Goh, “Hierarchical identity-based encryption with constant size ciphertext,” in EUROCRYPT 2005.Springer Berlin Heidelberg, 2005, pp.