IDENTITY BASED ENCRYPTION TRANSFORMATION FOR FLEXIBLE SHARING OF ENCRYPTED DATA IN PUBLIC CLOUD

P.Vijay Bhaskar Reddy, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India
K.Geetha, PG Scholar, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India

ABSTRACT: With the rapid development of cloud computing, more and more people and businesses in the public cloud share data. A data owner usually encrypts his data in such way as to safeguard the privacy of data stored in the cloud that select designated data users can decrypt the data. This poses a severe difficulty when the encrypted data is shared with more persons outside the data owner's initial names. In order to tackle this problem, we develop and define an IDBET model by smoothly merging two widely recognised encryption mechanisms, namely IDB encryption (IBE), and identity-based broadcast encryption (IBBE). IBET identifies and authorises data users to access data based on their recognisable identities, preventing burdensome certification management in common, secure distributed systems. More importantly, IBET provides an IBE ciphertext transformation method so that a new user group that is not defined by IBE encryption can access the underlying data. We construct an actual IBET system based on bilinear groups and demonstrate its security against strong attacks. The excellent efficiency and practicality of the proposed method are demonstrated by thorough theoretical and experimental investigations. Keywords: Cloud computing, Identity-based broadcast encryption, Public clouds.method are demonstrated by thorough theoretical and experimental investigations.

Keywords: Cloud computing, Identity-based broadcast encryption, Public clouds.

1. INTRODUCTION

Cloud storage is growing popularity recently. The demand for data outsourcing, which maintains organisational data, has increased in enterprise settings. Cloud storage is utilised as a back-up to numerous online services. File sharing or remote data access is now an easy task. Data users can utilise current wireless technologies to access all their data and emails from everywhere in the world through a mobile phone.In order to ensure data privacy, a usual technique is for the server to provide access rights after authentication, which implies that all data are disclosed via any unexpected access power. This gets significantly worse in a shared cloud computing environment. Data from various customers can be loaded to a single physical system on separate virtual machines. Another VM co-resident with the target can be stolen from data in a target VM. There are several cryptographic approaches to verify file availability that allow third parties to verify the existence of files without leaking or compromising.

2. RELATED WORK

Data protection is outsourced. In safe cloud-based information, cryptographic encryption techniques are typically employed. Traditional public-key encryption approaches are utilised for outsourcing user-focused access control. IDE is a promising solution for removing reliable certificates from users. Wei et al. employed IBE for data sharing on mobile computers. He and others used IBE to build a handshake system for patient safety. Broadcast identity encryption (IBBE) enhances the IBE to accommodate multi-receiver encryption users while encrypting a message. Deng et al. used IBBE to allow many authorised viewers to access the same outsourced file for the cloud system. A number of revokable schemes should be revoked by some IBBE recipients. Inter-domain transformation. Blaze et al. first used proxy encryption to manage their ciphertext transformation encryption systems.The PRE allows users to translate ciphertext from Alice into chip text under the public Bob password. Ateniese et al. defined PRE as interactive and non-interactive in different

Copyright @ 2021 Authors

categories, including PRE, Single Store and Multi Hop. Twin-way PRE. Much was done to improve PRE's safety and efficiency, in particular unidirectional PRE. Libert and Vergnaud have constructed the first one-way system. Cao et al suggested an independent PRE path to allow users to adopt a preference external visitor path. Guo al. introduced PRE proxy accounting unidirectional encryption key. Green and Ateniese offered the first PRE (IBPRE) ID, which would extend the PRE to PRE ID and IBE ID. Tseng and Chu introduced short code text IBPRE and decryption keys that can put confidential data holders at risk, i.e. the proxy server coalition and user access. This problem has been overcome by the revoked IBPRE cloud system Liang et al. The interaction between data proprietors and the processing authority of key generators is vital for the efficiency of this system.

3. SYSTEM ARCHITECTURE& ANALYSIS

SYSTEM ARCHITECTURE:

This image shows the architecture of our IBET system.An IBET system has four entities: data owners, data consumers, registri are cloud clients. RA is a trustworthy system setup party which answers to registration requests and outsourcing of file parameters. CSP undertakes two crucial tasks: 1) supply outsourced file storage services to consumers; 2) provide computer services to their customers in order to handle stored files. CSP storage and calculation services can be obtained in real-life by a company or organisation and the RA used as an IT centre by an organisation or company. Computers and storage are used by all (registered) personnel. This is permitted. Data owners might outsource the CSP data. IBE encryption may be employed by data holders for data processing and exporting to CSP for privacy protection the generated files (Chiphertext format). Assume that some data goes to an IBE encryption file (thus the data can be accessed by only one data consumer). If the data owner wants to communicate this data to other users, the data can be generated and forwarded to CSP, and then CSP can download data to a ciphertext file in IBBE ciphertext format. More data users can access previouslyEncrypted IBE information, which was first accessible to a single data user.

SYSTEM ANALYSIS:EXISTING SYSTEM

Wei et al. [7] used IBE in mobile computer contexts to secure data exchange. He et al. [8] used IBE to build a handshake method in the social network for the protection of patient data. Identity-based broadcast encryption (IBBE)[9] expands the IBE to provide multi-receiver crypting to the extent that the user once encrypts a message for several destination recipients. Deng et al.[10] used IBBE in the cloud storage systems to outsourced file in the light of such a desirable feature. A number of reverse IBBE algorithms are proposed to withdraw some recipients from the original IBBE ciphertext receiver list. Transformation inter-domain. Blaze et al. [15] originally introduced the concept of proxy reencryption in an encryption system for handling ciphertext transformation. This allows a user to transform a ciphertext generated under the public key of Alice into a ciphertext under the public key of Bob. Ateniese et al.[16] have categorised PRE as a two-way and one-way PRE, single hop and multihop PRE, interactive and non-interactive PRE, in different categories. There have been several initiatives to increase the efficiency and safety of PRE and most of them concentrate on unidirectional PRE. The first unidirectional PRE system was presented by Libert and Vergnaud[17]. Cao et al. [18] proposed the PRE autonomous path system to allow a user to choose the path to their outsourced data for preferred authorised visitors. Guo et al. [19] established unidirectional PRE accountability to identify a proxy that abusses its re-encryption keys. By merging PRE with IBE, Green and Ateniese[20] introduced the first ID-based PRE (IBPRE) as a PRE extension in ID settings. Chu and Tzeng[21] introduced an IBPRE method with short ciphertexts and decryption keys, however they may be vulnerable to collusion attacks, i.e. the proxy server coalition and authorised users could jeopardise sensitive knowledge about data holders. Liang et al. [22] resolved this security issue by presenting the revocable IBPRE cloud-based system. This approach demands the interaction between the data proprietors and the key generator authority for each transformation. By introducing IBBE in PRE Xu et al. [23] suggested an IBBEbased PRE scheme. Other PRE extensions, such as attribute-based PRE[24], [25], time-based PRE[26], functionbased

Copyright @ 2021 Authors

PRE[27], etc., are available in conjunction with IBPRE. However, essentially these PRE schemes translate ciphertexts into the same encryption system, i.e. not converting ciphertext into another format.

DISADVANTAGES

- In the existing work, the system does not provide Data integrity proof.
- thatis system is less performance due to lack of strong encryption techniques.

THE PROPOSED SYSTEM

The system does not provide data integrity proof in the existing work. Because of absence of robust encryption algorithms, this system is less efficient. In this article, the system has been constructed to answer the aforementioned question by investigating the transition of encryption between two different systems. For the first time, we present a new concept termed identity-based transformation in encrypting (IBET). We also define IBET's concept (including the definition of algorithms and security models). We then propose a concrete IBET system, which offers the following desirable properties in bilinear groups. • Identity-based data storage. The data owner can securely outsource their data to an untrusted remote cloud server. The data is encrypted and stored on the server in IBE/IBBE ciphertext format so that it is only accessible by the users permitted by the data owners. The unique identities of all users, including data holders and data consumers, eliminate the requirement of complicated public-key certificates.

• **Cross-domain encryption transformation**. Our IBET system achieves a cross-domain encryption process that can be seen as a connecting bridge IBE and IBBE. IBBE. In example, an IBBE ciphertext data owner (or approved data consumer) can convert the data stored in the IBE ciphertext format into data that can simultaneously access the data by an individual user indicated by the database owner (or authorised data consumer).

• **Strong security guarantee.** Our IBET programme provides a high level of safety that: 1) can deter unauthorised access to data stored in the cloud server; 2) it can prevent the leakage of some private information (e.g. private key) that authorises the transformation of encrypted data; 3) it does not reveal any useful information concerning sensitive data.

ADVANTAGES

- Data security protection: If data has been encrypted before outsourced, customers with correct decryption keys can only access it (these client are also called authorised clients).
- CSP or unauthorised clients cannot read the encrypted data (those having no correct decryption keys). Controllable transformation: CSP can only transform files defined by the data owner on the authorization token.
- In order to process undefined files or to discover sensitive data information encrypted in unspecifying file, CSP and other clients cannot collectively ex

4. PERFORMANCE EVALUATION

4.1 Theoretical Analysis

We total up the overhead computation for each algorithm on each side of the item in the table. The most costly cryptographic processes we take into account are exponentiations and bilinear maps. In the table, the time of evaluation for an exponentiation operation in G and a bilinear pairing were indicated by te and tp. The cost of calculating the RA installation procedure is linear in the maximum number m allowed for the users who can access the same data. RA just needs to make an exponentiation in G during the registration process to produce a private key. The Encrypt algorithm provides a data owner with two options of securing data. If the data owner wants just to access outsourced data by one (e.g. himself), the ciphertext for cases 1 is generated, which brings two exponentiations to him; if he wants to share data in the future with other users, he can generate the ciphertext for cases 2, taking four exponentiations. When the data owner determines the identities of

Copyright @ 2021 Authors

the customers who can access his data, the owner shall make an authorization token according to the cost n of these customers. The algorithms transform take one pair of CSPs to transform a file. The Decrypt algorithm uses a data consumer to decrypt an original file by using a bilinear pairing; the cost of the decrypt algorithm for a converted file is con consistent with a total number of allowed data consumers. Table 3 compares our IBET scheme with other relevant plans in terms of customer and CSP server storage costs and token generation calculation costs across bilinear groups, as well as some valuable features. Table, |Z according to the p|, |G|, |GT| indicate the length of the value in Z according to p, G and GT, respectively. Matsuo and Jiang et al. schemes support a multi-domain transformation that converts public key encryption system (PKE) files into IBE system files, but their schemes require the user of PKE to store public parameters (public keys) that are linear in size to the size (n) of destined data customers that can access their data.

The Identity based encryption approach achieved in Xu et al. and in our systems overcomes this efficiency issue. In comparison to Xu and others, our system demands that fewer public parameters are saved on the customer side and accomplishes a cross-domain identity transformation capability. This function removes the transformation limitation into a single encryption system. It also allows users to choose efficient identity-based data protection encryption mechanisms and transform encrypted data (if desired) so that users ofanother(IBBE) encryption system can access them.

computation complexity of each algorithm in the IBET schema

Algorithms	Computations	Entity
Setup	$(m+2)t_e + 1t_p$	RA
Register	$1t_e$	RA
Encrypt	$2t_e$ (case 1) or $4t_e$ (case 2)	Data owner
Authorize	$(n+4)t_e$	Data owner
Transform	$1t_p$	CSP
Decrypt	IBE: $1t_p$	Data consumer
	IBBE: $(n-1)\cdot t_e + 3t_p$	

4.2 Experimental Analysis We have carried out a series of experiments to evaluate the IBET's performance. Standford PBC library (http://crypto.stanford.edu/pbc/) uses bilined cryptographic procedures. The elliptical curve has type A (y2 = x3 + x), making p an element of 160 bits, and G an element of 256 bits. The details of our tests' hardware and software setups are listed in Table. We examined the performance of file creation and (original) access for the first time in the experiments. In particular, we have built the efficient BB04 IBE to compare its file creation and file access speed with ours. We also followed the principle of key encapsulation in reverse compatibility experiments. This means that first we utilised 256- bit AES symmetric keys to encrypt real data (about 1 KB) and then encrypted symmetrical keys via IBE. Therefore, the procedure of file access takes two steps: first to obtain the symmetrical keys and subsequently to retrieve data with the keys. Table demonstrates that BB04 IBE and our IBET systems require approximately the same times in creating files (approximately 60 msec) and accessing files (approximately 50 msec). Thus, while our IBET system introduces the mechanism for encryption translation, the file and file access methods most often utilised have not been modified.

Copyright @ 2021 Authors

TABLE III
COMPARISON WITH RELATED WORKS IN BILINEAR GROUPS

Schemes	Costs at Client side			Costs at CSP side		①	②	③
	Public parameters storage	Private key storage	Token computation	Original file storage	Transformed file storage			
Matsuo[28]	PKE: $3N\|\mathbb{Z}_p^*\|$ IBE: $4\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	PKE: $3\|\mathbb{Z}_p^*\|$ IBE: $2\|\mathbb{G}\|$	$1t_e$	$3\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	√	×	×
Jiang *et al.*[30]	PKE: $7N\|\mathbb{Z}_p^*\|$ IBE: $5\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	PKE: $2\|\mathbb{Z}_p^*\|$ IBE: $2\|\mathbb{Z}_p^*\|+1\|\mathbb{G}\|$	$6t_e+1t_p$	$4\|\mathbb{G}\|+3\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+2\|\mathbb{G}_T\|$	√	√	×
Xu *et al.*[23]	$(3m+2)\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	$1\|\mathbb{G}\|$	$(n+5)t_e$	$3\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	$4\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	×	√	√
Our IBET	$(m+1)\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	$1\|\mathbb{G}\|$	$(n+4)t_e$	$2\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	$4\|\mathbb{G}\|+1\|\mathbb{G}_T\|$	√	√	√

Notations: ① means cross-domain transformation; ② means non-interactive transformation; ③ means identity-based setting.

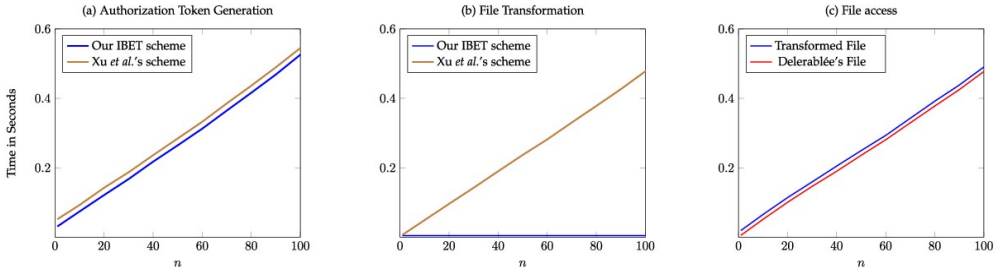

Fig. 4. Execution time of authorization token generation, File transformation and (transformed) file access.

5. CONCLUSION

In this article, we examined how encrypted data may be transformed securely and effectively in clouds. In order to deal with this problem, we presented an identity-based IBET model that would link the well-studied IBE and IBBE systems. IBET enables data owners to secure identity-based access controlled outsourced data, eliminating expensive cryptographic attestations for each user. IBET also provides data owners with a mechanism for the transformation of a cloud service provider (CSP) into IBBE-ciphertext file so that an authorised user may access the underlying data. We have proposed a practical IBET system that is safe from powerful attacks. Comprehensive experimental analyses show the efficiency and feasibility of the system.

6.REFERENCES

[1]"Cloud bulk data protection," PC, Vol. 45, No. 1, pp. 39–45, 2012.
[2] J. Yu, K. Ren, and C. Wang, "Enabling verifiable outsourcing of key updates for Cloud Storage Audits," IEEE Information Forensics and Security Transactions, vol. 11, no. 6, pp. 1362–75, 2016.
[3] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, "Safe, universal, and fine grain query results verifying the safe cloud data search system," IEEE Cloud Computing Transactions, 2017.
[4] K. Li, W. Zhang, C. Yang, and N. Yu, 'Cloud Encryption Search Security Analysis on a OneTomany Order,' IEEE Information Forensics and Security Transactions, vol. 10, no. 9, p. 1918– 1926, 2015.
[5] R. Zhang, R. Xue, and L. Liu, "Cloud Searchable Encryption: Survey," IEEE Computing Services Transactions, Vol. 11, No. 6: 978-996, 2018.
[6] D. Boneh and M. Franklin, "Because Pairing Identity-Based Encoding," Computing SIAM Journal, Vol. 32, No. 3, pp. 586–615, 2003.
[7] J. Wei, W. Liu, and X. Hu, "Secure Cloud Computing Data Sharing Using Revocable Storage Identity Crypt," IEEE Cloud Computing Transactions, 2016.
[8] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo and A. Vinel, IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, p. 633-0645, 2018: 'Probably-secure crossdomaine handshake with the symptoms-matching for the social health mobile network.' C. Delerabl'ee in International Conference on the theory and application of cryptology and information security, "Common identity broadcast encryption with constant ciphertexts and private keys."
[9] C. Delerabl'ee. Springer, 2007, pages 200-215.
[10] H. Deng, Q.Wu, B. Qin,W. Susilo, J. Liu, andW. Shi, "Asymmetric Cross-Crypto-System Encoding for Efficient and Safe Mobile Access to Sensitive Data," Proceedings at the 10th ACM Information, Computer and Communications Security Symposium. CJA, 2015, pp. 393-404.
[11]J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous file revoking identity-based encryption" in the Australasian Information Safety and Privacy Conference. 2016 Springer, pp. 223– 239.
[12] Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.

Copyright @ 2021 Authors