International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Identity-Based Encryption with Deployed Split in Cloud Computing

Melpakam Rohini Sudha[1], K.Somasehar[2]

[1]Department Of Mca, Rcr Institute Of Management And Technology, Tirupati, Andhra Pradesh, India

[2]Hod,Department Of Mca, Rcr Institute Of Management & Technology, Tirupati, Andhra Pradesh, India

ABSTRACT

In the basis of our existing system could be a novel cryptographical theme, specifically designed for pictures, named IES-CBIR. Key to its design is that the observation that in pictures, color information are often separated from texture information, enabling the utilization totally different|of various} encoding techniques with different properties for every one, and permitting privacypreserving Content-Based Image Retrieval to be performed by third-party, untrusted cloud servers.in existing system supported content we have a tendency to permitting users if the user is fake means that your data is hacked.so not only considering the content ,we have to consider another factor.to overcome this downside we have a tendency to move to planned model.in planned system we have a tendency to conseder identity based,in this based on identity we are permitting the user. during this paper, we have a tendency to introduce outsourcing computation into IBE revocation, and formalize the safety definition of outsourced revocable IBE for the primary time to the most effective of our data. we have a tendency to propose a theme to dump all the key generation connected operations throughout key-issuing and keyupdate, leaving only a constant number of simple operations for PKG and eligible users to perform domestically.In our theme, like the suggestion, we have a tendency to understand revocation through change the non-public keys of the unrevoked users. however not like that job that trivially concatenates period with identity for key generation/update and needs to re-issue the total non-public key for unrevoked users, we have a tendency to propose a unique collusion-resistant key supplying technique: we have a tendency to use a hybrid private key for every user, during which associate gate is concerned to attach and certain 2 sub-components, particularly the identity part and therefore the time part.At first, user is ready to get the identity part and a default time part (i.e., for current time period) from PKG as his/her non-public key in key-issuing. Afterwards, so as to keep up decryptability, unrevoked users must periodically request on keyupdate for time part to a recently introduced entity named Key Update Cloud Service supplier (KU-CSP).

Keywords: Identity-based encryption, Revocation, Outsourcing, Cloud computing.

I. INTRODUCTION

Identity-Based coding (IBE) is associate exciting substitute to public key coding, that is projected to create easier key managing during a certificate-based Public Key Infrastructure (PKI) by using humanintelligible characteristics (e.g., distinctive name, email address, IP address, etc) as public keys. Therefore, sender with IBE doesn't need to appear up public key and certificate, however overtly encrypts significance with receiver's identity. Consequently, receiver getting the non-public key connected with the resultant identity from private Key Generator (PKG) is ready to decrypt such cipher text. but IBE permits associate random string because the public key that is measured as likable recompense over PKI, it anxiety an original revocation instrument. Expressly, if the non-public keys of variety of users get compromised, we have a tendency to should provide a mean to cancel such users from system. In PKI setting, revocation mechanism is accomplished by appending lawfulness periods to certificates or using concerned mixtures of techniques. On the opposite hand, the awkward management of certificates is accurately the saddle that IBE strives to enhance. As way as we have a tendency to fathom, but revocation has been consistently calculated in PKI, few revocation mechanisms are branded in IBE In cycle with the enlargement of cloud computing, there has emerged the power for users to shop for on-demand computing from cloud-based services love Amazon's EC2 and Microsoft's Windows Azure. therefore it needs a replacement operating paradigm for introducing such cloud services into IBE revocation to mend the difficulty of potency and storage overhead delineated on top of. A naïve approach would be to easily get in the PKG's master to the Cloud Service suppliers (CSPs). The CSPs might then merely update all the non-public keys by mistreatment the normal key update technique and transmit the private keys back to unrevoked users. However, the naive approach is predicated on associate fantastic assumption hat the CSPs are totally sure and is allowed to access the master for IBE system. On the contrary, in apply the general public clouds are seemingly outside of identical sure domain of users and square measure curious for users' individual privacy. For this reason, a challenge on the way to style a secure revokable IBE theme to cut back the overhead computation at PKG with associate entrusted CSP is raised. during this paper, we have a tendency to introduce outsourcing computation into IBE revocation, and formalize the safety definition of outsourced revokable IBE for the primary time to the most effective of our information. we have a tendency to propose a theme to offload all the key generation connected operations throughout key-issuing and key-update, going only a continuing range of easy operations for PKG and eligible users to perform locally. In our theme, like the suggestion in [4], we have a tendency to understand revocation through updating the non-public keys of the unrevoked users. however not like that work [4] that trivially concatenates period of time with identity for key generation/update and needs to reissue the entire non-public key for unrevoked users, we have a tendency to propose a unique collusion-resistant key supply technique: we have a tendency to use a hybrid non-public key for every user, within which associate AND circuit is concerned to attach and sure 2 sub-components, particularly the identity element and also the time element. At first, user is ready to get the identity element and a default time element (i.e., for current time period) from PKG as his/her private keying key-issuing. Afterwards, so as to keep up decode ability, unrevoked users has to sporadically request on keyupdate foretime element to a recently introduced entity named Key Update Cloud Service supplier (KU-CSP).Compared with the previous work [4], our theme doesn't have to be compelled to re-issue the entire non-public keys, however simply got to update a light-weight element of it at a specialised entity KU-CSP. we have a tendency to conjointly specify that 1) with the help of KU-CSP, user wants to not contact with PKG in key-update, in alternative words, PKG is allowed to be offline when causation the revocation list to KU-CSP. 2) No secure channel or user authentication is needed throughout key-update between user and KU-CSP. what is more, we have a tendency to deliberate to understand revokable IBE with a semi honest KU-CSP. to attain this goal, we have a tendency to gift a security increased construction underneath the recently formalized Refereed Delegation of Computation (RDoC) model [7]. Finally, we offer in depth experimental results to demonstrate the potency of our planned construction. Identity-based coding associate IBE theme which generally involves 2 entities, PKG and users (including sender and receiver) is consisted of the following four algorithms. Setup(λ) : The setup algorithm takes as input a security parameter λ and outputs the public key PK and the master key MK. Note that the master is unbroken secret at PKG. KeyGen(MK, ID) : The non-public key generation rule is travel by PKG, which takes as input the master key MK and user's identity ID ∈ ∗ . It returns a non-public key SKID appreciate the identity ID. Encrypt (M,ID) : The coding rule is travel by sender, that takes as input the receiver's identity automatic data processing and a message M to be encrypted. It outputs the cipher text CT.Decrypt (CT,SKID_) : The coding rule is travel by receiver, that takes as input the cipher text CT and his/her private key SKID_ . It returns a message M or an error.

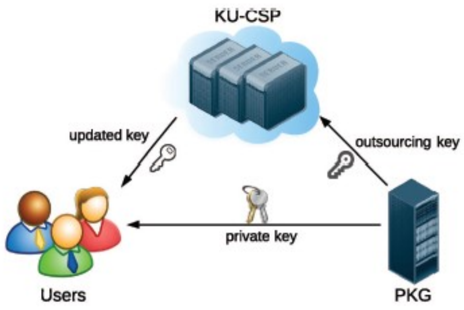

Fig. 1. System Model for IBE with Outsourced Revocation

MODULES:

1. User
2. KU-CSP
3. PKG
4. Key-Distribution

MODULES DESCRIPTION:

USER:

The User Module is responsible for the file sharing process with the cloud. The whole process includes three types of key distributions. The Private Key will be shared from PKG to the user. Once the outsourced key is received at the KU-CSP, then it will trigger the updated key distribution to the users with respect to the details received from the users end such as users ID, Mail ID, File Details. Finally the user is associated with the File Download process as well with the collaboration of updated key and Private key distribution.

KU-CSP:

KU-CSP provides computing service in the Infrastructure as a service (IaaS) model, which provides the raw materials of cloud computing, such as processing, storage and other forms of lower level network and hardware resources in a virtual, on demand manner via the Internet. Differing from traditional hosting services with which physical servers or parts thereof are rented on a monthly or yearly basis, the cloud infrastructure is rented as virtual machines on a per-use basis and can scale in and out dynamically, based on customer needs.

It is responsible for updating key to user as per the users request.

PKG:

PKG has to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. We employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing.

Key Distribution:

At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decryptability, unrevoked users needs to periodically request on key update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

II. CONCLUSION

In this paper, focusing on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable theme during which the revocation operations are delegated to CSP.

With the help of KU-CSP, the proposedscheme is full-featured: 1) It achieves constant efficiency for each computation at PKG and private key size at user; 2) User needs not to contact with PKG during key-update, in alternative words, PKG is allowed to be offline once causing the revocation list to KU-CSP; 3) No secure channel or user authentication is needed throughout key-update between user and KU-CSP. Furthermore, we consider to understand revocable IBE under a stronger adversary model. we tend to present a sophisticated construction and show it's secure underneath RDoC model, during which a minimum of one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs interact, it's unable to help such user re-obtain his/her decryptability. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

III. REFERENCES

[1]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology-CRYPTO'98. Springer, 1998.

[2]. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3]. F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.

[4]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology-CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA: ACM, 2008, pp. 417–426.

[6]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557.

[7]. R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Report 2011/518, 2011.

[8]. U. Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC '97. New York, NY, USA: ACM, 1997, pp. 506–516.

[9]. S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.

[10]. R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 37–61.

[11]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in 17th European Symposium on Research in Computer Security (ESORICS), 2012.

[12]. M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications

Security, ser. ASIACCS ’10. New York, NY, USA: ACM, 2010, pp. 48–59.

[13]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology-CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin / Heidelberg, 1985, vol. 196, pp. 47–53.

[14]. C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 2001, vol. 2260, pp. 360–363.

[15]. R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology EUROCRYPT 2003, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin / Heidelberg, 2003, vol. 2656, pp. 646–646.

[16]. D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2004, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds. Springer Berlin / Heidelberg, 2004, vol. 3027, pp. 223–238.

[17]. "Secure identity based encryption without random oracles," in Advances in Cryptology-CRYPTO 2004, ser. Lecture Notes in Computer Science, M. Franklin, Ed. Springer Berlin / Heidelberg, 2004, vol. 3152, pp. 197–206.

[18]. B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 114–127.

[19]. C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2006, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin / Heidelberg, 2006, vol. 4004, pp. 445–464.

[20]. C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proceedings of the 40th annual ACM symposium on Theory of computing, ser. STOC ’08. New York, NY, USA: ACM, 2008, pp. 197–206.