International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 6, Issue 8, August 2017, pp.801-805, ISSN 2278 -1412

Secure and Efficient Implementation of Identity Based Encryption in Cloud Computing

Yogesh Kumar Darwai[1], Vimal Shukla[2]
[1]M.Tech Scholar, Department of Cyber Security, Kailash Narayan Patidar College of Science &Technology, Bhopal, India;
[2]Head of Department, Department of Cyber Security , Kailash Narayan Patidar College of Science &Technology, Bhopal, India;
Email: [1]ykd1806@gmail.com, [2]vimalshukla.cse@gmail.com;

Abstract *– In our scheme, like the suggestion, we tend to understand revocation through change the private keys of the unrevoked users. however not like that work that trivially concatenates period of time with identity for key generation/update and needs to re-issue the entire private key for unrevoked users, we tend to propose a completely unique collusion-resistant key issue technique: we tend to use a hybrid private key for every user, during which an AND gate is concerned to connect and bound 2 sub-components, specifically the identity part and also the time component. Moreover, we tend to consider realizing revocable IBE with a semi-honest KU-CSP. To realize this goal, we tend to present a security increased construction under the recently formalized Refereed Delegation of Computation (RDoC) model.*

Keywords*: Outsourcing, Private Key Generator, Cloud Server Provider, Cloud Computing, Identity-based encryption, Key Distribution.*

I. Introduction

With the advancement of information and computing technology, large-scale datasets are being exponentially generated today. Examples under various application contexts include medical images, remote sensing images, satellite image databases, etc. Along with such data explosion is the fast-growing trend to outsource the image management systems to cloud and leverage its economic yet abundant computing resources too efficiently and effectively attain, store, and distribute images from data owners to a large number of data users. Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.

I.1. What is cloud computing?

Cloud computing is that the employ of computing resources (hardware and software) that are transport as a service above a network (typically the Internet). The name comes from the common use of a cloud-shaped image as an concept for the advanced infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's information, software package and computation. Cloud computing consists of hardware and software package resources created accessible on the net as managed third-party services. These services usually offer access to advanced software package applications and high-end networks of server computers.

I.2. How Cloud Computing Works?

The purpose of cloud computing is to apply usual supercomputing, or high-performance computing power, in general used by military and investigate facilities, to execute tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers normally running low-cost consumer PC technology with specialized connections to spread data-processing tasks across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

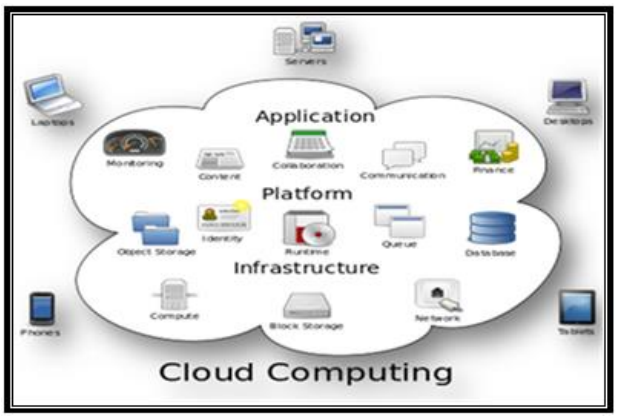

Fig.1 Structure of cloud computing

II. System Design

A cloud computing design by combining with an example that a company uses a cloud to change its staffs inside a similar group or department to share files. The system model consists of three totally different entities: Key Update Cloud Service Provider, private key and user as illustrated in Fig.2.

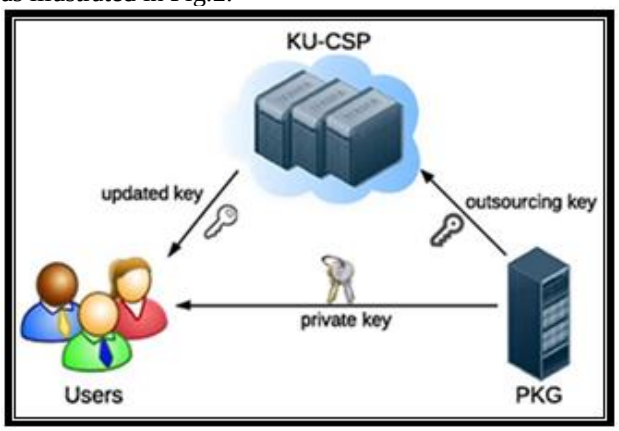

Fig. 2: System Design

II.1. 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.

II.2. 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.

II.3. 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.

III. Proposed Methodology

- In this proposed work, introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for PKG and eligible users to perform locally.
- In our scheme, as with the suggestion, we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: 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. 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).

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is

generated by this system. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

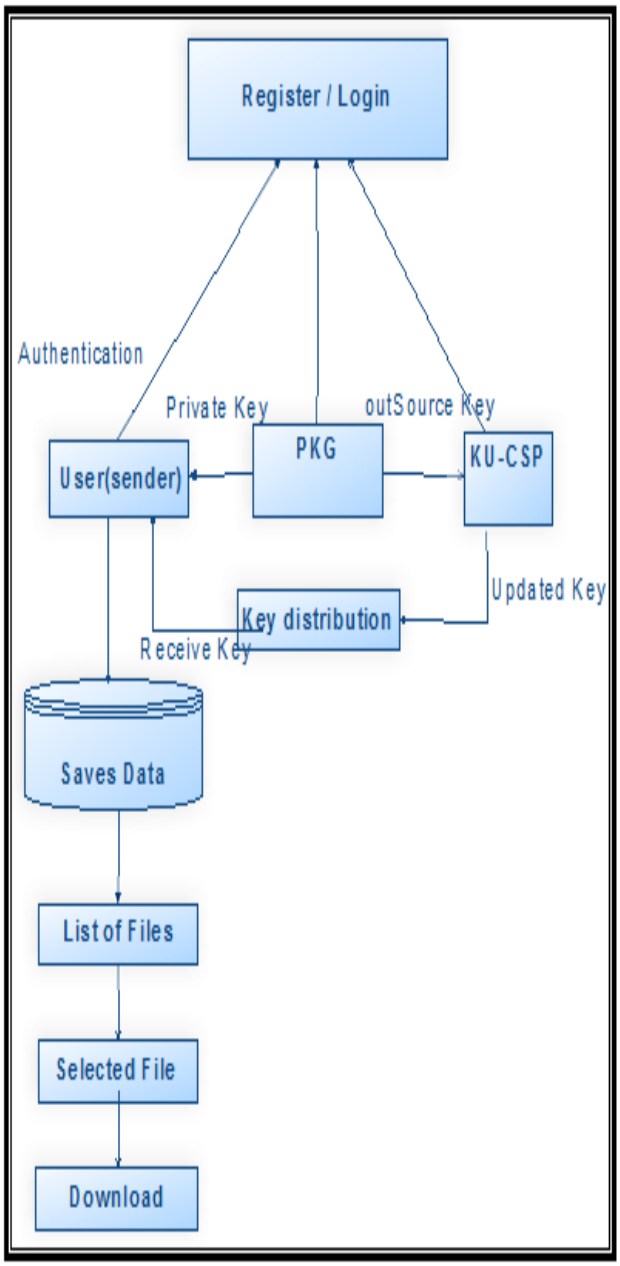

Fig.3 data flow diagram of system design

IV. Result

Fig.4 user login page

Fig.4 shows the user login after registered the user,

Fig.5 user home page

Fig.5shows the user home page.

Fig.6 uploads data in cloud server

Fig.6 shows the upload data in cloud server. In this we upload the any data file upload in cloud server.

Fig.7 Send outsource key panel

Fig.7 shows send outsource key panel. PKG will send the outsourced key to CSP.

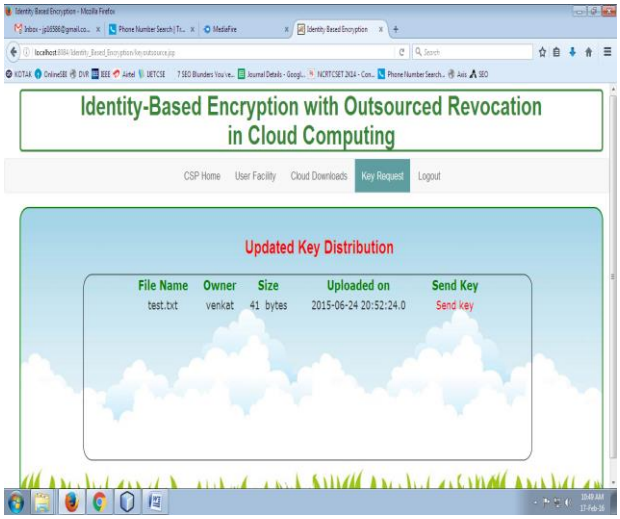

Fig.8 Update key Distribution

Fig.8 based on the trigger the CSP will receive the outsourced key from PKG then CSP sends the updated key to the users' registered mail id.

Fig.9 Cloud download panel

Fig.9 shows download data in cloud server.

V. Conclusion

In this proposed work introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for PKG and eligible users to perform locally. In this research work, propose a revocable scheme in which the revocation operations are delegated to Cloud Service Provider. With the aid of key update Cloud Service Provider, the proposed scheme is full-featured: It achieves constant efficiency for both computation at private key generate and private key size at user; User needs not to contact with private key generate during key update, in other words, private key generate is allowed to be offline after sending the revocation list to key update Cloud Service Provider.

References

[1] Li, Jin, et al. "Identity-based encryption with outsourced revocation in cloud computing." Ieee Transactions on computers 64.2 (2015): 425-437.

[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 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'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, vol. 2947, pp. 375–388.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun. Security (CCS'08), 2008, pp. 417–426.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 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, Rep. 2011/ 518, 2011 [online]. Available: http://eprint.iacr.org/2011/518.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM Symp. Theory Comput. (STOC'97), 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography TCC'05), 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, A. Smith, Ed. Berlin, Germany: Springer, 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 Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.

[12] M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 48–59.
[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.
[14] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, B. Honary, Ed. Berlin/ Heidelberg: Springer, 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'03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.