Survey on Identity-Based Encryption with Outsourced Revocation in Cloud Computing

Shruti Kirti Dixit [1], Dr. Tripti Arjariya[2]

[1]M.Tech Scholar, Department of Computer Science Engineering, Bhabha Engineering Research Institute Bhopal shaludixit4@gmail.com, India;

[2], HOD, Department of Computer Science Engineering, Bhabha Engineering Research Institute Bhopal, tripti.beri@gmail.com, India;

***Abstract** – In this research work, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. In this paper many research papers are surveyed related to the Identity-Based Encryption with Outsourced Revocation in Cloud Computing. In this present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model.*

***Keywords**: Identity-based encryption (IBE), revocation, outsourcing, cloud computing,*

I. Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform 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.

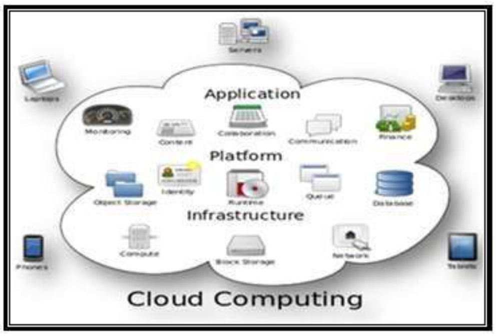

Fig.1 Structure of cloud computing

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores 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.

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

• On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

• Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

• Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

• Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

• Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

II. Literature Survey

Jin Li et. al [1] "Identity-based Encryption with Outsourced Revocation in Cloud Computing", in this paper focusing on the critical issue of identity revocation, authors introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU CSP, the proposed scheme is full-featured: 1) It achieves constant efficiency for both computation at PKG and private key size at user; 2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP.

Cong Wang et. al [2] "Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud", in this paper proposed OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. OIRS exploits techniques from different domains, and aims to take security, design complexity, and efficiency into consideration from the very beginning of the service flow. With OIRS, data owners can utilize the benefit of compressed sensing to consolidate the sampling and image compression via only linear measurements. Data users, on the other hand, can leverage cloud's abundant resources to outsource the image recovery related `1 optimization computation, without revealing either the received compressed samples, or the content of the recovered underlying image. Besides its simplicity and efficiency, authors show OIRS is able to achieve robustness and effectiveness in handling image reconstruction in cases of sparse data as well as non-sparse general data via proper approximation. Both extensive security analysis and empirical experiments have been provided to demonstrate the privacy-assurance, efficiency, and the effectiveness of OIRS. On top of the current architecture, authors also demonstrate a proof-of-concept of possible performance speedup through hardware built-in system design, which authors believe is our important future work to be pursued.

Jin Li et. al [3] "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption", in this paper propose an efficient attribute-based access control system in cloud computing. In our system, two CSPs namely KG-CSP and D-CSP are introduced as employees to finish the outsourced heavy tasks for user management and file access respectively. The overhead at both users and attribute authority sides is thus being minimized. A challenging issue in the proposed system is how to outsource the computational task to CSPs without any private information leakage. To deal with this issue, authors formulize an underlying primitive namely OABE and provide several OABE constructions with outsourced key issuing and decryption. Finally, through extensive experiments, it demonstrates that our OABE construction achieves efficient key-issuing and decryption at AA and user sides respectively.

Jingwei Li et. al [4] "Outsourcing Encryption of Attribute-Based Encryption with MapReduce", in this paper formulize the paradigm of outsourcing encryption of ABE in cloud computing. authors utilize MapReduce to propose a security enhanced construction which is secure under the assumption that the master node as well as at least one of the slave nodes in cloud is honest. Another advantage of the proposed construction is that it is able to delegate encryption for any access policy, instead of a special hybrid access policy. With our proposed outsourcing method, the computational cost at user side in encryption algorithm is reduced to four exponentiations, which is constant and does not grow with the number of attributes included in the cipher text.

D. Benjamin et al.[5] "Private and cheating-free outsourcing of algebraic computations", authors give protocols for the secure and private outsourcing of linear algebra computations, that enable a client to securely outsource expensive algebraic computations (like the multiplication of huge matrices) to two remote servers, such that the servers learn nothing about the customer's private input or the result of the computation, and any attempted corruption of the answer by the servers is detected with high probability. The computational work done locally by the client is linear in the size of its input and does not require the client to carry out locally any expensive encryptions of such input. The computational burden on the servers is proportional to the time complexity of the current practically used algorithms for solving the algebraic problem (e.g., proportional to n3 for multiplying two times matrices). If the servers were to collude against the client, then they would only find out the client's private inputs, but they would not be able to corrupt the answer without detection by the client.

C. Wang et al.[6] "Secure and practical outsourcing of linear programming in cloud computing", Cloud computing enables customers with limited computational resources to outsource large-scale computational tasks to the cloud, where massive computational power can be easily utilized in a pay-per-use manner. However, security is the major concern that prevents the wide adoption of computation outsourcing in the cloud, especially when end-user's confidential data are processed and produced during the computation. Thus, secure outsourcing mechanisms are in great need to not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by validating the computation result. Such a mechanism of general secure computation outsourcing was recently shown to be feasible in theory, but to design mechanisms that are practically efficient remains a very challenging problem. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. In order to achieve practical efficiency, our mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate security/efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation. In particular, by formulating private data owned by the customer for LP problem as a set of matrices and vectors, authors are able to develop a set of efficient privacy-preserving problem transformation techniques, which allow customers to transform original LP problem into some random one while protecting sensitive input/output information. To validate the computation result, authors further explore the fundamental duality theorem of LP computation and derive the necessary and sufficient conditions that correct result must satisfy. Such result verification mechanism is extremely efficient and incurs close-t- - o-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.

III. Method

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.

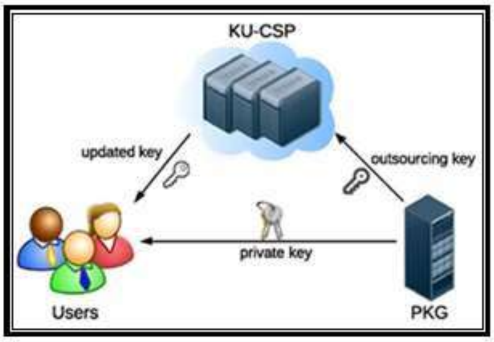

Fig.2 System Design

III.1. Modules Description

A. 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.

B. 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.

C. 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.

D.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).

IV. 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 paper basic system design are explained and discuss about different module description.

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] Wang, Cong, et al. "Privacy-assured outsourcing of image reconstruction service in cloud." IEEE Transactions on Emerging Topics in Computing 1.1 (2013): 166-177.

[3] Li, Jin, et al. "Fine-grained access control system based on outsourced attribute-based encryption." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2013.

[4] Li, Jingwei, et al. "Outsourcing encryption of attribute-based encryption with mapreduce." International Conference on Information and Communications Security. Springer, Berlin, Heidelberg, 2012.

[5] Benjamin, David, and Mikhail J. Atallah. "Private and cheating-free outsourcing of algebraic computations." Privacy, Security and Trust, 2008. PST'08. Sixth Annual Conference on. IEEE, 2008.

[6] Wang, Cong, Kui Ren, and Jia Wang. "Secure and practical outsourcing of linear programming in cloud computing." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[7] Zhou, Zhibin, and Dijiang Huang. "Efficient and secure data storage operations for mobile cloud computing." Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, 2012.

[8] Green, Matthew, Susan Hohenberger, and Brent Waters. "Outsourcing the decryption of abe ciphertexts." USENIX Security Symposium. Vol. 2011. No. 3. 2011.

[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] Thilakanathan, Danan, et al. "Secure data sharing in the Cloud." Security, Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg, 2014. 45-72.