An Efficient Certificate less Encryption for Secure Data Sharing In Public Clouds

Ayat Hekmat Lateef
Master of Computer Science
University College of Science, Osmania University, Hyderabad, India
Al Yarmouk University College, Diyala, Baghdad, Iraq

Abstract:

The study proposes a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificate less public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations. The study apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully decrypt the partially decrypted data using their private keys. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. We also propose an extension to the above approach to improve the efficiency of encryption at the data owner. The study implements our mCL-PKE scheme and the overall cloud based system, and evaluates its security and performance. Our results show that our schemes are efficient and practical.

Keywords: *Certificateless encryption, Decryption, mCL-PKE, public key encryption, Security.*

Introduction

DUE TO the benefits of public cloud storage, organizations have been adopting public cloud services such as Microsoft Skydrive and Dropbox to manage their data. However, for the widespread adoption of cloud storage services, the public cloud storage model should solve the critical issue of data confidentiality. That is, shared sensitive data must be strongly secured from unauthorized accesses. In order to assure confidentiality of sensitive data stored in public clouds, a commonly adopted approach is to encrypt the data before uploading it to the cloud. Since the cloud does not know the keys used to encrypt. The data, the confidentiality of the data from the cloud is assured. However, as many organizations are required to enforce fine-grained access control to the data, the encryption mechanism should also be able to support finegrained encryption based access control. A typical approach used to support finegrained encryption based access control is to encrypt different sets of data items to which the same access control policy applies with different symmetric keys and give users either the relevant keys or the ability to derive the keys. Even though the key derivation-based approaches reduce the number of keys to be managed, symmetric key based mechanisms in general have the problem of high costs for key management. In order to reduce the overhead of key management, an alternative is to use a public key cryptosystem. However, a traditional public key cryptosystem requires a trusted Certificate Authority (CA) to issue digital certificates that bind users to their public keys. Because the CA has to generate its own signature on each user's public key and manage each user's certificate, the overall certificate management is very expensive and complex. To address such shortcoming, Identity-Based Public Key Cryptosystem (IBPKC) was introduced, but it suffers from the key escrow problem as the key generation server learns the private keys of all users. Recently, Attribute Based Encryption (ABE) has been proposed that allows one to encrypt each data item based on the access control policy applicable to the data. However, in addition to the key escrow problem, ABE has the revocation problem as the private keys given to existing users should be updated whenever a user is revoked. In order to address the key escrow problem in IB-PKC, Al-Riyami and Paterson introduced a new cryptosystem called Certificateless Public Key Cryptography (CL-PKC).

RELATED WORK:

Knowledge engineering (KE) was defined in 1983 by Edward Feigenbaum, and Pamela McCorduck as follows: KE is an engineering discipline that involves integrating knowledge into computer systems in order to solve complex problems normally requiring a high level of human expertise. At present, it refers to the building, maintaining and development of knowledge-based systems. It has a great deal in common with software engineering, and is used in many computer science domains such as artificial intelligence, including databases, data mining, expert systems, decision support systems and geographic information systems. Knowledge engineering is also related to mathematical logic, as well as strongly involved in cognitive science and socio-cognitive engineering where the knowledge is produced by socio-cognitive aggregates (mainly humans) and is structured according to our understanding of how human reasoning and logic works. In this work, we exhibit Eucalyptus - an open-source programming structure for Distributed computing that actualizes what is usually alluded to as framework as an Administration (IaaS); frameworks that give clients the capacity to run and control wholevirtual machine occurrences conveyed over an assortment physical assets. We diagram the essential standards of the Eucalyptus outline, point of interest imperative operational parts of the framework, and talk about engineering exchange offs that we have made with a specific end goal to permit EUCALYPTUS to be versatile, particular and easy to use on foundation ordinarily found inside scholarly settings. At long last, we give confirm that EUCALYPTUS empowers clients acquainted with existing matrix and HPC frameworks to investigate new distributed computing usefulness while keeping up access to existing, well known application advancement programming and network middleware.

Bitar, N., Gringeri, S., & Xia, T. J. (2013), research says cloud today confront a few difficulties when facilitating line-of-business applications in the cloud. Fundamental to a large number of these difficulties is the restricted backing for control over cloud system capacities, for example, the capacity to guarantee security, execution sureties or separation, and to adaptably intervene middleboxes in application organizations. In this paper, we show the configuration and usage of a novel cloud organizing framework called CloudNaaS. Clients can influence CloudNaaS to convey applications expanded with a rich and extensible arrangement of system capacities, for example, virtual system seclusion, custom tending to, administration separation, and adaptable intervention of different middleboxes. CloudNaaS primitives are specifically executed inside the cloud framework itself utilizing fast programmable system components, making CloudNaaS very productive. We assess an OpenFlow-based model of CloudNaaS and observe that it can be utilized to instantiate a mixed bag of system capacities in the cloud, and that its execution is hearty even despite huge quantities of provisioned administrations and connection/gadget disappointments.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August), cloud computing has raised IT as far as possible by offering the business environment information stockpiling and limit with adaptable versatile figuring preparing energy to match flexible request and supply, whilst lessening capital use. However the open door expense of the fruitful execution of Cloud registering is to successfully deal with the security in the cloud applications. Security cognizance and concerns emerge when one starts to run applications past the assigned firewall and move closer towards the general population space. The motivation behind the paper is to give a general security point of view of Cloud processing with the expect to highlight the security worries that ought to be appropriately tended to and figured out how to understand the maximum capacity of Cloud registering. Gartner's rundown on cloud security issues, also the discoveries from the International Data Corporation venture board study in view of cloud dangers, will be examined in this paper.

Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008, June) research says mobile phones keep on approaching the capacities and extensibility of standard desktop PCs. Shockingly, these gadgets are likewise starting to face a large number of the same security dangers as desktops. As of now, portable security arrangements reflect the conventional desktop display in which they run identification benefits on the gadget. This methodology is complex and asset concentrated in both processing and force. This paper proposes another model whereby versatile antivirus usefulness is moved to an off-gadget system administration utilizing various virtualized malware location motors. Our contention is that it is conceivable to spend data transfer capacity assets to essentially lessen on-gadget CPU, memory, and force assets. We show how our incloud model improves portable security and decreases on-gadget programming unpredictability, while taking into consideration new administrations, for example, stage particular behavioral examination motors. Our benchmarks on Nokia's N800 and N95 cell phones demonstrate that our portable specialists devours a request of greatness less CPU and memory while likewise expending less power in like manner situations contrasted with existing on-gadget antivirus programming.

Certificate less Public Key Cryptography

At right on time stages Functional encryption permits one to encode a discretionary complex access control approach with the encrypted message. Attribute based encryption (ABE) presented by Sahai and Waters is a more expressive predicate encryption with a public index.

Next Introduce Functional encryption permits one to encode a discretionary complex access control approach with the encrypted message. At that point Al-Riyami and Paterson presented a

Certificateless Public Key Cryptography (CL-PKC). Since every client holds a blend of KGC delivered halfway private key and an extra user-chosen secret, the key escrow issue can be determined. Since the coming of CL-PKC, numerous CLPKE plans have been proposed in view of bilinear pairings. The computational expense needed for pairing is still significantly high contrasted with standard operations such as modular exponentiation in finite fields.

Secure Searchable Encryption

At earlier stage, Single Keyword Searchable Encryption Customary single decisive word searchable encryption schemes typically build an encoded searchable list such that its content is covered up to the server unless it is given suitable trapdoors produced by means of secret key(s). Next Comes the Boolean Keyword Searchable Encryption to advance search functionalities, conjunctive keyword search over encoded data have been proposed. These plans bring about substantial overhead created by their major primitives, for example, reckoning cost by bilinear guide, for instance, or correspondence cost by secret sharing, for instance, . As a more general search methodology, predicate encryption plans are as of late proposed to backing both conjunctive and disjunctive search.

Trust Management with our SMTP Gateway

You can now utilize Protected Trust to encrypt and send mechanized messages with the Protected Trust SMTP handoff. For instance, you could coordinate your charging framework to email receipts through the Protected Trust SMTP transfer and they will get encrypted before being conveyed to the end beneficiary. Alternately, you could send robotized arrangement updates to your patients in a protected, HIPAA-agreeable way. This can be performed by virtually any stage making incalculable conceivable utilization cases. Your application associate with the Protected Trust SMTP Relay utilizing TLS encryption and logs as a part of with an Access Credential. When the record is verified, the hand-off sweeps the message body for a <protectedtrust> XML tag. The XML piece is then parsed and if no mistakes are discovered, the email is encrypted and sent through Protected Trust to the beneficiaries utilizing the tagged confirmation technique.

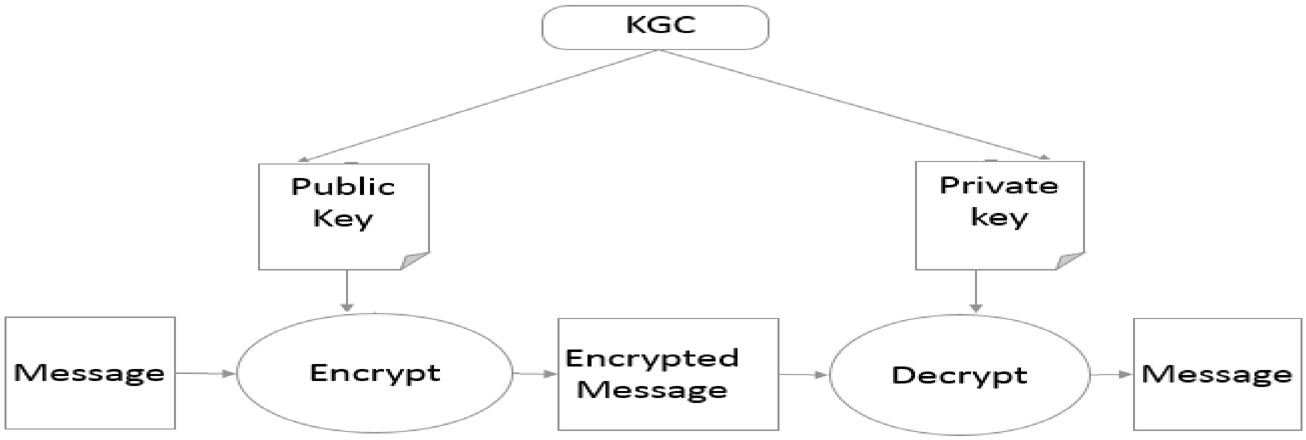

Figure 1: Public-key cryptography

Proposed System

Our methodology helps immediate revocation and guarantees the confidentiality of the data stored away in an untrusted public cloud while upholding the access control approaches of the data owner. Further, for various users satisfying the same access control approaches, our enhanced methodology performs just a single encryption of every data set and diminishes the general overhead at the data owner.

Privacy-Preserving and Secure Cloud Storage

It is essential to perceive that if one specifically applies our fundamental mCL-PKE plan to cloud computing and if numerous clients are approved to get to the same data, the encryption costs at the information owner can get to be high. The cloud is used for trust management which act as secure storage as well as a key generation center (KGC) and secure indexing agent for encrypted data. In proposed system first user generate his own public and private key in order to authenticate with cloud by using secure access control policies and share the credential and public key to key generation center (KGC). On next step the cloud generate key for encrypting owner data, In this paper, shockingly, we characterize and tackle the issue of multi-keyword ranked search over encrypted cloud data (MRSE) while protecting strict framework shrewd security in the cloud computing standard. Among different multi-keyword semantics, we pick the proficient closeness measure of "direction matching," i.e., whatever number matches as would be prudent, to catch the importance of information reports to the inquiry question. In particular, we utilize "inward item closeness", i.e., the quantity of inquiry pivotal words showing up in an archive, to quantitatively assess such comparability measure of that document to the search query.

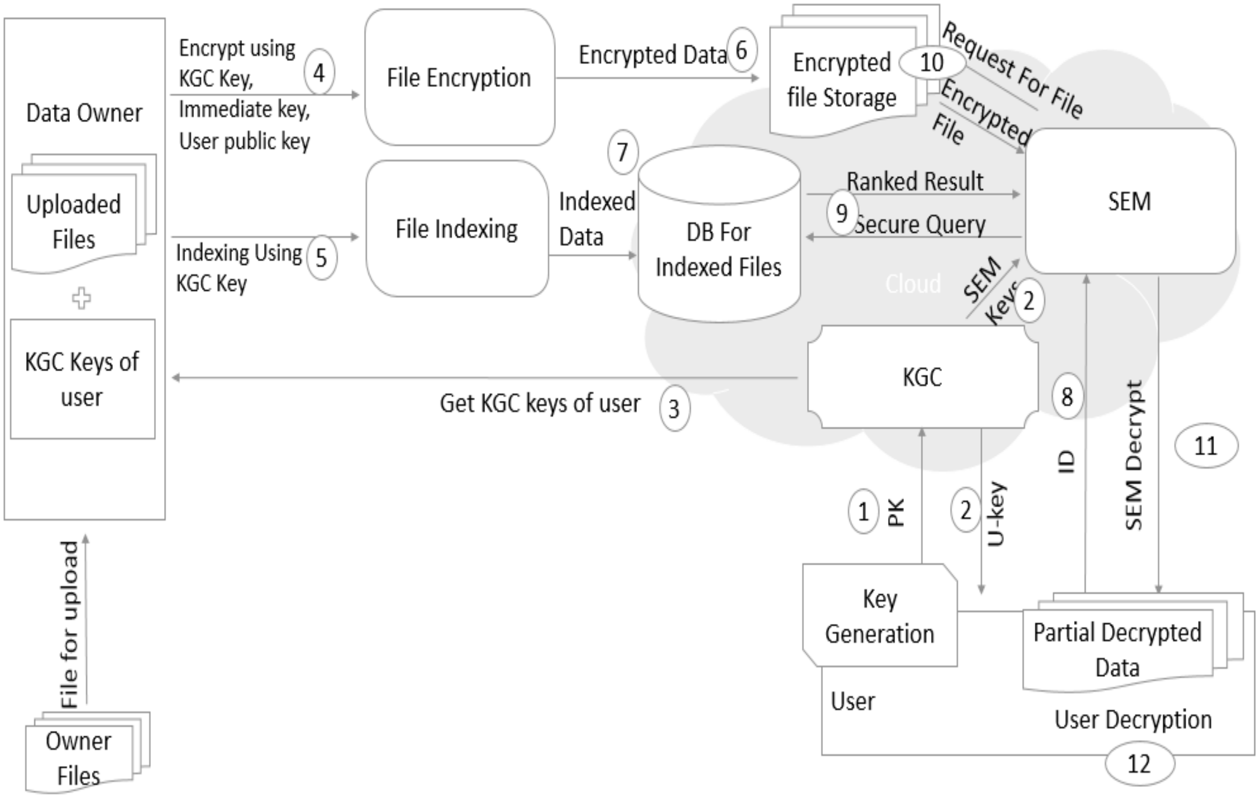

Figure 2: System Architecture

In this section, we present the mediated Certificateless Public Key Encryption (mCL-PKE) scheme and its security model. Then, we prove the formal security of mCL-PKE scheme.

The mediated certificateless public key encryption (mCL-PKE**) scheme** is a 7-tuple mCL-PKE= (SetUp,SetPrivateKey, SetPublicKey, SEM-KeyExtract, Encrypt,SEM-Decrypt, USER-Decrypt).

The Computational Diffie-Hellman (CDH) problem is defined as follows: Let p and q be primes such that $q| (p - 1)$. Let g be a generator of $Z*p$. Let A be an adversary. A tries to solve the following problem: Given (g, g^a, g^b) for uniformly chosen a, b, c ∈ $Z*q$, compute k = gab. We define A's advantage in result of CDH problem by **Adv (A)** =Pr [A $(g, g^a, g^b) = g^{ab}$].

CONCLUSION

In this paper we have proposed the first mCL-PKE scheme without pairing operations and provided its formal security. Our mCL-PKE solves the key escrow problem and revocation problem. Using the mCL-PKE scheme as a key building block, we proposed an improved approach to securely share sensitive data in public clouds. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted public cloud while enforcing the access control policies of the data owner. Our experimental results show the efficiency of basic mCL-PKE scheme and improved approach for the public cloud. Further, for multiple users satisfying the same access control policies, our improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner. If a user is revoked, the data owner updates the access control list at the SEM so that future access requests by the user are denied. If a new user is added to the system. The data owner encrypts the data using the public key of the user and uploads the encrypted data along with the updated access control list to the cloud. Note that existing users are not affected by revoking or adding users to the system. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted public cloud while enforcing the access control policies of the data owner. Our experimental results show the efficiency of basic mCL-PKE scheme and improved approach for the public cloud. Further, for multiple users satisfying the same access control policies, our improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

REFERENCE:

1. Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008, June). Virtualized in-cloud security services for mobile devices. In Proceedings of the First Workshop on Virtualization in Mobile Computing (pp. 31-35). ACM.
2. Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., ... & Zeghlache, D. (2011). Challenges for cloud networking security. In Mobile Networks and Management (pp. 298-313). Springer Berlin Heidelberg.
3. Bitar, N., Gringeri, S., & Xia, T. J. (2013). Technologies and protocols for

data center and cloud networking. Communications Magazine, IEEE, 51(9), 24-31.

4. Houidi, I., Mechtri, M., Louati, W., & Zeghlache, D. (2011, July). Cloud service delivery across multiple cloud platforms. In Services Computing (SCC), 2011 IEEE International Conference on (pp. 741-742). IEEE.
5. Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009, May). The eucalyptus open-source cloud-computing system. In Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on (pp. 124-131). IEEE.
6. Wodczak, M. (2011, November). Resilience aspects of autonomic cooperative communications in context of cloud networking. In Network Cloud Computing and Applications (NCCA), 2011 First International Symposium on (pp. 107-113). IEEE.
7. Bitar, N., Gringeri, S., & Xia, T. J. (2013). Technologies and protocols for datacenter and cloud networking. Communications Magazine, IEEE, 51(9), 24-31.
8. Bechler, M., Hof, H. J., Kraft, D., Pahlke, F., & Wolf, L. (2004, March). A cluster-based security architecture for ad hoc networks. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies (Vol. 4, pp. 2393-2403). IEEE.
9. Covington, M. J., Fogla, P., Zhan, Z., & Ahamad, M. (2002). A context-aware security architecture for emerging applications. In Computer Security Applications Conference, 2002. Proceedings. 18th Annual (pp. 249-258). IEEE.
10. Zhou, L., & Chao, H. C. (2011). Multimedia traffic security architecture for the internet of things. Network, IEEE, 25(3), 35-40.