IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-7 E-ISSN: 2347-2693

Leakage-Resilient Cryptosystem with Efficient and Flexible Key Delegation in Scalable Cloud Storage

M.sarika[1], J.Sasikiran[2],* L.Sunitha[3] , D. KoteswaraRao[4]

[1]M.Tech Scholar, Vidya Vikas Institute of Technology, Chevella, Telangana
[2]Professor, CSE Department, Vidya Vikas Institute of Technology, Chevella, Telangana
[3]Associate Professor, CSE Department, Vidya Vikas Institute of Technology, Chevella, Telangana
[4]Associate Professor, CSE, Vidya Vikas Institute of Technology, Chevella, Telangana

www.ijcseonline.org

Received: Jun/09/2015 Revised: Jun/28/2015 Accepted: July/18/2015 Published: July/30/ 2015

Abstract: We present a generic construction of a public key encryption scheme that is resilient to key leakage from any hash proof system. The construction does not rely on additional computational assumptions, and the resulting scheme is as efficient as the underlying hash proof system. Existing constructions of hash proof systems imply that our construction can be based on a variety of theoretic assumptions. We achieve leakage-resilience under the respective static assumptions of the original systems in the standard model, while also preserving the efficiency of the original schemes.

Key terms: Public Key, Hash Proof, Encryption, Aggregate Key

1. INTRODUCTION

Data sharing is an important functionality in cloud storage. 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 provide access to advanced software applications and high-end networks of server computers. Here, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems [2] that produce constant size cipher texts such that efficient delegation of decryption rights for any set of cipher texts is possible. The novelty is that one can aggregate any set of secret keys [3][4] and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible [11] choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

2. LITERATURE SURVEY

2.1 SPICE: Simple Privacy-Preserving Identity-Management for Cloud Environment: Identity security and privacy [1] have been regarded as one of the top seven cloud security threats. There are a few identity management solutions proposed recently trying to tackle these problems. However, none of these can satisfy all desirable properties. In particular, unlink ability ensures that none of the cloud service providers (CSPs), even if they collude, can link the transactions of the same user. On the other hand, delegatable authentication is unique to the cloud platform, in which several CSPs may join together to provide a packaged service, with one of them being the source provider which interacts with the clients and performs authentication while the others will be transparent to the clients. Note that CSPs may have different authentication mechanisms [7] that rely on different attributes. Moreover, each CSP is limited to see only the attributes that it concerns. It presents SPICE – the first digital identity management system that can satisfy these properties in addition to other desirable properties. The novelty of this scheme stems from combining and exploiting two group signatures so that we can randomize the signature to make the same signature look different for multiple uses of it and hide some parts of the messages which are not the concerns of the CSP. This scheme is quite applicable to cloud systems due to its simplicity and efficiency.

2.2 Privacy- Preserving Public Auditing for Secure Cloud Storage: Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications[5] and services from a shared pool of

configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability[6] for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities [17] toward user data privacy, and introduce no additional online burden to user a secure cloud storage system supporting privacy-preserving public auditing. Extend the result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. TPA preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

3. PROPOSED WORK

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner's anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality.

A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff.

Proposed System

We study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts[15], without increasing its size. Specifically, our problem statement is "To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decrypt able by a constant-size decryption key (generated by the owner of the master-secret key)." We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. That means the cipher texts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher text classes. The extracted key have can be an aggregate key which is as compact as a secret key for a single class.

- The delegation of decryption can be efficiently implemented with the aggregate key.

4. IMPLEMENTATION

key-aggregate cryptosystem is implemented through 4 phases

1. System Model
2. Key Generation
3. Encryption
4. Aggregate Key Transfer

4.1System Model

- Data Owner: In this module we executed by the data owner to setup an account on an untrusted server. On input a security level parameter 1^{λ} and the number of cipher text classes n (i.e., class index should be an integer bounded by 1 and n), it outputs the public system parameter(param), which is omitted from the input of the other algorithms for brevity.
- Network Storage: With our solution, User1 can simply send User2 a single aggregate key via a secure e-mail. User1 can download the encrypted photos from User2 Drop box space and then use this aggregate key to decrypt these encrypted photos. In this Network Storage is untrusted third party server.

4.2 Key Generation

- Public-key cryptography, also known as asymmetric cryptography[8], is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.
- The public key is used to encrypt plaintext whereas the private key is used to decrypt cipher text .Data owner to randomly generate a public/master-secret key[19] pair.

4.3 Encryption

- Encryption keys also come with two flavours symmetric key or asymmetric (public) key. Using symmetric encryption, when Alice wants the data to be originated from a third party, she has to give the

encrypted her secret key; obviously, this is not always desirable.

- By contrast, the encryption key and decryption key are different in public key encryption. The use of public-key encryption gives more flexibility for our applications.

4.4 Aggregate Key Transfer

- A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen.
- Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher text classes via Extract.
- The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt.

5. CONCLUSION

Protecting user's data privacy is very important in cloud storage. In this paper, we consider how to "compress" secret keys in public-key cryptosystems which support group of secret keys for different cipher text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key allocation which can only save spaces if all key-holders share a similar set of privileges.

A limitation in our work is the predefined bound of the number of maximum cipher text classes. In cloud storage, the number of cipher texts usually grows dynamically. So we have to reserve enough cipher text classes for the future extension. Otherwise, we need to expand the public-key. Although the parameter can be downloaded with cipher texts, it would be better if its size is independent of the maximum number of cipher text classes. On the other hand, when one carries the delegated keys around in a mobile device without using specific trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

6. ACKNOWLEDGEMENTS

I would like to express my cordial thanks to Sri. CA. BashaMohiuddin, Chairman, Smt. Rizwana Begum-Secretary and Sri. Touseef Ahmed-Vice Chairman, Dr.M.Anwarullah, Principal - Farah Group of Institutions, Hyderabad for providing moral support, encouragement and advanced research facilities. Authors would like to thank the anonymous reviewers for their valuable comments. And they would like to thank Dr.V. Vijaya Kumar, Anurag Group of Institutions for his invaluable suggestions and constant encouragement that led to improvise the presentation quality of this paper.

7. REFERENCES

[1]. M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. **2009**.

[2]. T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption," Proc. 10th Int'l Conf. Cryptology and Network Security (CANS '11), pp. 138-159, **2011**.

[3]. R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 185-194, **2007**.

[4]. C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," Proc. Information Security Conf. (ISC '07), vol. 4779, pp. 189-202, **2007**.

[5]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, **2003**.

[6]. M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, **2009**.

[7]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, **2009**.

[8]. F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, **2007**.

[9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 89-98, **2006**.

[10]. S.G. Akl and P.D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. Computer Systems, vol. 1, no. 3, pp. 239-248, **1983**.

[11]. G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, 316-322, **1989**.
[12]. G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes,"J. Cryptology, vol. 25, no. 2, pp. 243-270, **2012**.
[13]. R.S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95-98, **1988**.
[14]. Y. Sun and K.J.R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," Proc. IEEE INFOCOM '04, **2004**.
[15]. Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," Proc. IEEE Global Telecomm. Conf. (GLOBECOM '04), pp. 2067-2071, **2004**.
[16]. J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," technical report, Microsoft Research, **2009**.
[17]. B. Alomair and R. Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication," J. Universal Computer Science, vol. 15, no. 15, pp. 2937-2956, **2009**.
[18]. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, **2001**.
[19]. Ratheesh , Jogesh A Visual Cryptographic Scheme For Owner Authentication Using Embedded Shares ,Indian Journal of Computer Science and Engineering (IJCSE) ,ISSN : 0976-5166 Vol. 5 No.5 Oct-Nov **2014**, pgno:190-195
[20]. S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple As-sumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, **2010**.
[21]. F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575, pp. 392-406, **2007**.

AUTHOR PROFILE

Ms. M. Sarika Graduated inB.Tech [CSE]from JNTU Hyd. Pursuing Masters Degree in M.Tech [CSE] from Vidya Vikas Institute of Technology, Chevella, affiliated to JNT University, Hyderabad. Her area of interests include Network security, Compiler Design and Cloud Computing & Big Data.

Dr. J. Sasi Kiran Graduated in B.Tech [EIE] from JNTU Hyd. He received Masters Degree in M.Tech [CSE] JNT University, Hyderabad. He received Ph.D degree in Computer Science from University Of Mysore, Mysore. At Present he is working as Professor in CSE and Dean – Administration in Vidya Vikas Institute of Technology, Chevella, R.R. DistTelangana State, India. His research interests include Image Processing, Data Mining and Network Security. He has published 39 research papers till now in various National, International Conferences, Proceedings and Journals. He has received best Teacher award twice from Vidya Group, Significant Contribution award from Computer Society of India and Passionate Researcher Trophy from Sri. Ramanujan Research Forum, GIET, Rajuhmundry, A.P, India.

L. Sunitha Graduated from kakatiya university Warangal received her M.Tech in Computer Science and Engineering from JNTU, Hyderabad in 2009. She has 15 years of teaching experience, presently she is working as Associate Professor in Vidya Vikas Institute of Technology Chevella, R.R. Dist Telangana State, India and also pursuing PhD in Computer Science and Engineering from JNTU Hyderabad, India. . She has received best Teacher award from Vidya Group .Her area of specialization is Data mining. Member in CSI and IAENG, she has published many papers in various National, International conferences Proceedings and Journals.

D. Koteswara Rao Graduated in B.Tech CSE fromJNTUHyd. He received Masters Degree in M.Tech [CSE] from Nagarjuna University, Guntur. Currently he is working as Associate Professor in vidya vikas institute of Technology R.R. Dist Telangana State, India. His research interests include Formal Languages and Automata Theory. He has published research papers in various National, International Conferences, Proceedings and Journals. He has received best Teacher award from Vidya Group.