IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

An Effective Hierarchical Key Management System Using Elliptic Curve Cryptography And Session Key Establishment On Cloud

Preetha V

Department of Computer Science and Engineering
Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

Nisha Soms

Department of Computer Science and Engineering
Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

Abstract- **Content Delivery Network (CDN) on clouds normally communicate with authenticated subscribers using HTTPS to provide privacy and data integrity. The SSL private key is the most critical component in secure communication, and it can be even more important than the protected content itself. Here the key challenge is how to provide security guarantees so that the SSL private key and the content can be stored onto untrusted public clouds. To solve this issue, keys are generated in Key Distribution Centre(KDC) using Elliptic Curve Cryptographic algorithm and the private key will be hidden even to the CDN and cached or stored in the Key Sub-Centres. Only when decrypting the content or any request from the user, CDN will get the private key cached from the Key Sub-Centres. This type of key management approach in our paper is named as Effective Hierarchical Key Management System. In this system session keys will also be generated for further authentication. In this project a web application will be developed, with a dummy CDN(i.e. Content Delivery Network and KDC(Key Distribution Centre) in that users can be registered, registered users alone will be able to request the CDN and the private key will be secured in the KDC. Once this key authentication gets success user can be able to manage his files in the cloud like upload files to the cloud or download file from the cloud.**

Keywords—Key management, Cloud, CDN (Content Delivery Network), KDC (Key Distribution Centre)

I. Introduction

In the recent decades, cloud-based storage service [15], [17], [22] has attracted considerable attention from both academia and industries. It may be widely used in many Internet-based commercial applications (e.g., Apple iCloud) due to its long-list benefits including access flexibility and free of local data management. Increasing number of individuals and companies nowadays prefer to outsource their data to remote cloud in such a way that they may reduce the cost of upgrading their local data management facilities/devices. However, the worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service.

In many practical applications, outsourced data may need to be further shared with others. For example, a Dropbox user Alice may share photos with her friends. Without using data encryption, prior to sharing the photos, Alice needs to generate a sharing link and further share the link with friends. Although guaranteeing some level of access control over unauthorized users (e.g., those are not Alice's friends), the sharing link may be visible within the Dropbox administration level (e.g., administrator could reach the link). Since the cloud (which is deployed in an open network) is not be fully trusted, it is generally recommended to encrypt the data prior to being uploaded to the cloud to ensure data security and privacy. One of the corresponding solutions is to directly employ an encryption technique (e.g., AES) on the outsourced data before uploading to cloud, so that only specified cloud user (with valid decryption key) can gain access to the data via valid decryption.

To prevent shared photos being accessed by the "insiders" of the system, a straightforward way is to designate the group of authorized data users prior to encrypting the data. In some cases, nonetheless, Alice may have no idea about who the photo receivers/users are going to be. It is possible that Alice only has knowledge of attributes with respect to photo receivers. In this case, traditional public key encryption (e.g., Paillier Encryption), which requires the encryption to know who the data receiver is in advance, cannot be leveraged. Providing policy-based encryption mechanism over the outsourced photos is therefore desirable, so that Alice makes use of the mechanism to define access policy over the encrypted photos to guarantee only a group of authorized users is able to access the photos.

II. Cloud Computing

Cloud computing, [11], [12], [15], [17], or something being in the cloud, is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact is served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user—arguably, rather like a cloud. The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location.

2.1 Advantages –

Cloud computing [11], [12], [21], [22], [24] relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically re-allocated per demand. This can work for allocating resources to users. For example, a cloud computer facility, which serves European users during European business hours with a specific application (e.g. email) while the same resources are getting reallocated and serve North American users during North America's business hours with another application (e.g. web server). This approach should maximize the use of computing powers thus reducing environmental damage as well since less power, air conditioning, rack space, etc. is required for a variety of functions. The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model to the OPEX model.

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.

2.2. Management Challenges –

Cloud computing [21], [22], [24] presents a number of management challenges. Companies using public clouds do not have ownership of the equipment hosting the cloud environment, and because the environment is not contained within their own networks, public cloud customers don't have full visibility or control. Users of public cloud services must also integrate with an architecture defined by the cloud provider, using its specific parameters for working with cloud components. Integration includes tying into the cloud APIs for configuring IP addresses, subnets, firewalls and data service functions for storage. Because control of these functions is based on the cloud provider's infrastructure and services, public cloud users must integrate with the cloud infrastructure management.

Capacity management is a challenge for both public and private cloud environments because end users have the ability to deploy applications using self-service portals. Applications of all sizes may appear in the environment, consume an unpredictable amount of resources, and then disappear at any time.

Hybrid cloud environments, which combine public and private cloud services, sometimes with traditional infrastructure elements, present their own set of management challenges. These include security concerns if sensitive data lands on public cloud servers, budget concerns around overuse of storage or bandwidth and proliferation of mismanaged images.

III. Existing System

Cryptography [8], [18], [32] is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. Problem here is if the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's private key will decode it. Nowadays these asymmetric cryptographic methods are used in the Cloud Computing too. The private key is the most critical component in secure communication, and it can be even more important than the protected content itself if the private key is stolen in the untrusted environment like cloud, files will also be stolen and the total trust on the cloud will be lost. The disadvantage of this system is that if the private key is stolen in the cloud then the total trust on the cloud will be lost.

IV. Proposed System

Content Delivery Network (CDN) on clouds normally communicates with authenticated subscribers using HTTPS to provide privacy and data integrity. The SSL private key is the most critical component in secure communication, and it can be even more important than the protected content itself. Here the key challenge is how to provide security guarantees so that the SSL private key and the content can be stored onto untrusted public clouds. To solve the issue, keys are generated in Key Distribution Centre (KDC) using Elliptic Curve Cryptographic algorithm and the private key will be hidden even to the CDN and cached or stored in the Key Sub-Centres. Only when decrypting the content or any request from the user, CDN will get the private key cached from the Key Sub-Centres. This type of key management approach in our paper is named as Effective Hierarchical Key Management System. In this system session keys will also be generated for further authentication.

In this proposed work, a web application will be developed, with a dummy CDN (i.e. Content Delivery Network and KDC (Key Distribution Centre) in that users can be registered, registered users alone will be able to request the CDN and the private key will be secured in the KDC. Once this key authentication gets success user can be able to manage his files in the cloud like upload files to the cloud or download file from the cloud. For storage of the files uploaded by the user cloud storage application called Dropbox is used. Dropbox is a public Software-as-a-Service (SaaS) cloud application. The main advantage is that this approach guarantees the security of the private key even from the CDN (i.e., recipient).

V. Elliptic Curve Cryptographic Algorithm(ECC)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,
E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)

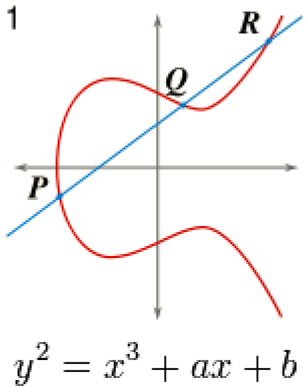

Figure 1 Simple Elliptic Curve

5.1. ECC Key Generation –

A public key Q = (xQ,yQ) associated with a domain parameter (q, a, b, G, n, h) is generated for an entity A using the following procedure :

- Select a random or pseudo-random integer d in the interval [1, n-1].
- Compute Q = dG.
- A's public key is Q; A's private key is d.

5.2. ECC Key Validation –

A public key Q = (xQ,yQ) associated with a domain parameter (q, a, b, G, n, h) is validated for an entity A using the following procedure :

- Check that Q ≠ O
- Check that xQ and yQ are properly represented elements of GF (q).
- Check that Q lies on the elliptic curve defined by a and b.
- Check that nQ = O.

5.3. Advantages of ECC –

- Very fast key generation
- Smaller keys, cipher-texts, and signatures
- Moderately fast encryption and decryption

This method is harder to crack since there is no known solution to the mathematical problem given by the equation producing the elliptical curve in a graph. Therefore, only one way remains for hackers: a brute-force attack — or a trial-and-error approach, in other words. This complexity makes ECC more secure compared to RSA.

VI. KEY GENERATION

Key generation [4], [32] is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number 'd' within the range of 'n'. Using the following equation, we can generate the public key

$$Q = d * P \qquad (1)$$

Where d is the random number that we have selected within the range of (1 to n-1) and it acts as the private key. P is the point on the curve, Q is the public key and d is the private key.

6.1. Encryption –

Let 'm' denote the message that we are sending. We have to represent this message on the curve. These have in-depth implementation details. All the advance research on ECC is done by a company called Certicom.
Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].
Two cipher texts, C1 and C2 will be generated as follows:

$$C1 = k*P \qquad (2)$$

$$C2 = M + k*Q \qquad (3)$$

C1 and C2 will be sending.

6.2. Decryption –

We have to get back the message 'm' that was send to us,

$$M = C2 – d * C1 \qquad (4)$$

M is the original message that we have send.

6.3. Proof –

M = C2 – d * C1

C2 – d * C1 = (M + k * Q) – d * (k * P)

(C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P

(Canceling out k * d * P)

= M (Original Message)

VII.CONCLUSION

The secure data sharing between user and Cloud resources is implemented using Elliptic curve cryptography and session key management. Thus, our approach Effective Hierarchical Key Management System will guarantee the security of the private key by generating keys in Key Distribution Centre (KDC) using Elliptic Curve Cryptographic algorithm and the private key will be hidden even to the CDN and cached or stored in the Key Sub-Centres. Only when decrypting the content or any request from the user, CDN will get the private key cached from the Key Sub-Centres. As the future work, have to upload, encrypt, download and decrypt the files after the validation of the above-mentioned process.

REFERENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin, “Charm: a framework for rapidly prototyping cryptosystems”, Journal of Cryptographic Engineering, 3(2):111–128, 2013.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata, “Innovative technology for cpu based attestation and sealing”, In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] Alexandros Bakas and Antonis Michalas, “Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX”, In SecureComm 2019, pages 472–486, 2019.

[4] Amos Beimel, “Secure schemes for secret sharing and key distribution”, PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[5] John Bethencourt, Amit Sahai, and Brent Waters, “Ciphertext-policy attribute-based encryption”, In S&P 2007, pages 321–334. IEEE, 2007.

[6] Victor Costan and Srinivas Devadas, “Intel SGX Explained”, IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov “IRON: functional encryption using Intel SGX”, In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto, “Secure integration of asymmetric and symmetric encryption schemes”, In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, “Attribute-based encryption for fine-grained access control of encrypted data”, In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au, “Improving privacy and security in decentralized ciphertext-policy attribute-based encryption”, IEEE transactions on information forensics and security, 10(3):665–678, 2015.

[11] Christofer Hoff, “Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of sustainability)” http://www. rationalsurvivability.com/blog/?p=66.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson “Attribution of fraudulent resource consumption in the cloud”, In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[13] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen, “Intel R software guard extensions: Epid provisioning and attestation services”, White Paper, 1:1–10, 2016.

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado, “Inferring fine-grained control flow inside sgx enclaves with branch shadowing”, In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe, “Outsourced attribute based encryption with keyword search function for cloud storage”, IEEE Transactions on Services Computing, 10(5):715–725, 2017.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han, “Full verifiability for outsourced decryption in attribute based encryption”, IEEE Transactions on Services Computing, DOI:10.1109/TSC.2017.2710190, 2017.

[17] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong. Tmacs, “A robust and verifiable threshold multi-authority access control system in public cloud storage”, IEEE Transactions on parallel and distributed systems, 27(5):1484–1496, 2016.

[18] Ben Lynn et al., “The pairing-based cryptography library. Internet: crypto”, stanford. edu/pbc/[Mar. 27, 2013], 2006.

[19] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar, “Innovative instructions and software model for isolated execution”, In HASP@ISCA 2013, page 10, 2013.

[20] Antonis Michalas, “The lord of the shares: combining attribute based encryption and searchable encryption for flexible data sharing”, In SAC 2019, pages 146–155, 2019.

[21] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei, “Auditable σ-time outsourced attribute-based encryption for access control in cloud computing”, IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.

[22] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei, “White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively”, IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.

[23] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong Lin, “Large universe ciphertext-policy attribute-based encryption with white-box traceability”, In Computer Security-ESORICS 2014, pages 55–72. Springer, 2014.

[24] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei, “Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud”, In Computer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[25] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and Xiaodong Lin, “White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes”, IEEE Transactions on Information Forensics and Security, 10(6):1274–1288, 2015.

[26] Olga Ohrimenko, Felix Schuster, C´edric Fournet, Aastha Mehta, Sebastian Nowozin, Kapil Vaswani, and Manuel Costa, “Oblivious multi-party machine learning on trusted processors”, In USENIX Security Symposium, pages 619–636, 2016.

[27] Ashay Rane, Calvin Lin, and Mohit Tiwari, “Raccoon: Closing digital side-channels through obfuscated execution”, In 24th USENIX Security Symposium, USENIX Security 2015, pages 431–446, 2015.

[28] Phillip Rogaway, “Authenticated-encryption with associated-data”, In Proceedings of the 9th ACM conference on Computer and communications security, pages 98–107, ACM, 2002.

[29] Amit Sahai and Brent Waters, “Fuzzy identity-based encryption. In Advances in Cryptology”, EUROCRYPT 2005, pages 457–473, Springer, 2005.

[30] Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado, “T-SGX: Eradicating controlled-channel attacks against enclave programs”, In NDSS 2017, 2017.

[31] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado, “Inferring fine-grained control flow inside sgx enclaves with branch shadowing”, In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

[32] Xiaokang Hu, Jian Li, Changzheng Wei, Weigang Li, Xin Zeng, Ping Yu and Haibing Guan, “STYX: A Hierarchical Key Management System Oriented to Elastic Content Delivery Networks on Public Clouds”, 2019.