

A SECURE DATA SHARING IN PUBLIC CLOUDS WITH INDEPENDENT KEY GENERATION USING ELLIPTIC CURVE CRYPTOGRAPHY SCHEME

Dr. C Nalini¹, R.G. Suresh²

¹Professor, Computer Science and Engineering,
BIST, BIHER, Bharath University, Chennai – 73.

²Research Scholar, Computer Science and Engineering, Vels University
nalini.cse@bharathuniv.ac.in

ABSTRACT

Cloud computing is an emerging economic and computing paradigm with the development of Internet technology. Various application services can be provided to satisfy user's requirements by the cloud computing. One of cloud computing application services commonly used is data storage, and users can outsource their storage and store their sensitive data in the cloud. In this paper, we propose an Elliptic Curve Cryptography (ECC) scheme with Session mediator and Key Generation Center. The session mediator provides the validation of any decryption key for both the user and data owner respectively. The time fraction is being set for the decrypting the data by a single key for any user. The Key Generation Center is playing a vital role for generating the Encryption and Decryption key for the data owner and user encrypt and decrypt the data before uploading in the cloud and downloading from the cloud. This will bring vulnerabilities in the secure key generation. A new method is discovered to implement the key generation centre as independent center and share keys independently. This method will provide an efficient and secure key generation between the user, data owner and the cloud environment.

Keywords: Session Mediator, Key Generation Center, Elliptic Curve Cryptography.

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to the shared pool of configurable computing resources networks, storage, servers, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction[1-6]. A public cloud is one based on the standard cloud computing paradigm, where a cloud service provider makes numerous resources like servers and storage, available globally over the web. Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organizations hoping to gain profit. People love to share information with one another. Due to all these advantages of the public cloud many of the organizations are now use the public cloud to store the data. But there are some problems with this public cloud. The

most challenging problem faced by the public cloud is the confidentiality of its sensitive data. But the major drawback of this system is the key management. In order to avoid this drawback this system introduced a mediated certificate less encryption method for the secure data sharing. But this system doesn't assure the confidentiality of the data. It only guarantees the protocol will work properly. So here a new approach is introduced to assure the confidentiality of the sensitive data in the cloud. 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[7-9].

Certificate less Public Key Encryption scheme reduces the key management. In this scheme, user's private key consists of a secret value chosen by the user and a partial private key generated by the Key Generation Center (KGC). If any user compromised the cloud, using its private key

attempts to access the data in the cloud[10-16]. The scheme was found to be insecure. Cloud service meaning that stored data should not result to any clear data to the cloud service provider. This is possible through symmetrically encrypting the data before storing the data in cloud itself, enforcing the data security in cloud by not exposing the symmetric key to the cloud. Key management is another tedious issue that we come across. Data access control in the cloud leads to an security concerns which is provide an main research goal to the researchers and developer of cloud computing. The main goal of the project is to provide a privacy and security concern for the cloud storage data owner when they are outsourcing their confidential data to the public cloud.. Proposed technique Elliptic Curve Cryptography (ECC) is providing the better

enhancement in compare to the existing technique. The ECC (Elliptic curve cryptography) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The proposed technique is generating the encryption and decryption key for both user and Data owner respectively by the key generation center. Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the data with public key and the user will decrypt its private key. The session mediator is proving the intermediate key for the encrypting and decrypting the data over the cloud and doing a perfect management for validating the key validation time within the side of data owner and user[17-21].

2. RELATED WORK

Bhavesh Rahulkar and Praveen Shende proposed 'A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing'[22-26]. In this scheme Two Layer Encryption means Double Encryption for securely outsourcing the data in cloud. This scheme solves key escrow problem and Data Reveal problem by RSA algorithm of asymmetric key approach. In existing mCL-PKE scheme there is Certificate-less Encryption and also single encryption and it is half decrypted by the „CLOUD“ and remaining half is decrypted by the „USER but in my scheme there will be certification for the User and two layer encryptions. The outer layer encryption will be decrypted by the „CLOUD“ and Inner layer encryption will be fully decrypted by the „USER only, By this manner the data/information will be highly secured. My Aim is "To Secure the „TEXT Data Items of the Data-Owner by Double Encryption in Cloud Computing". this project conclude, The scheme of double encryption and certification of the users provide high security to the data, and asymmetric key approach (RSA) is very easy in key distribution. The future enhancement of this scheme is that RSA can also be used for performing digital signature and it will be helpful for improving the security in future.

Seung-Hyun Seo Mohamed Nabeel Xiaoyu Ding Elisa Bertino, Fellow proposed 'An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds'. This paper propose a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in

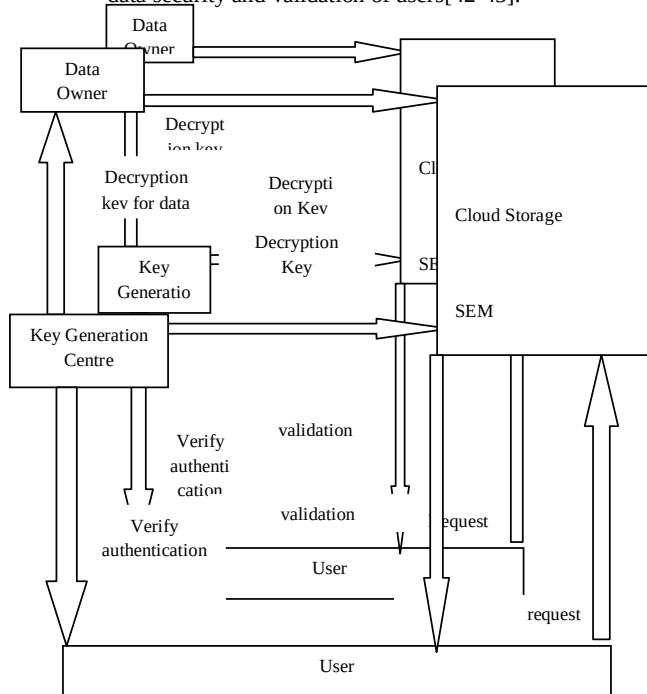
public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations 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. We 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[27-30].

3. PROPOSED METHODOLOGY

The popularity and widespread use of Cloud have brought great convenience for data sharing and collection. Data sharing with a large number of participants must take into account several issues, including efficiency[31-35], data integrity and privacy of data owner. The shared data must be strongly secured from

unauthorized accesses.

The common approach to ensure confidentiality is to encrypt the data before uploading it to the cloud. Many encryption mechanisms support fine-grained encryption based access control. In our proposed scheme, first data owner register on cloud. Then data owner upload data on cloud[36-41]. Cloud receives the data and put ECC encryption on data. Elliptic Curve Cryptography (ECC) is providing the better enhancement in compare to the existing technique. Protection of data is achieved by this step. After successful encryption key generation center sent the decrypt key to Data Owner. Now the user process will start. In that first user register on cloud and request the cloud to access data. Once cloud gets the request from user it validates the user by the user information. If user is valid person, key generation center sends decrypt key to user at the same time it send decryption key information and data information to Session Mediator (SEM Keys). Session Mediator is responsible for maintaining the user session and provides the security on data. Users can decrypt the data using the decryption key. Users can use the data depend on the type of data. Because session mediator gives the accessibility to users depend on the data. If user time limit is exceeds session mediator close the connection of user session. In this proposed system we achieve the data security and validation of users[42-45].



3.1 Data Owner Registration and User Registration

The Data Owner registers with the cloud to upload the data in the cloud storage system. User registers with the cloud to access data.

3.2 Data Encryption

Before uploading the data in the cloud the data is encrypted using Elliptic Curve Cryptography (ECC) algorithm. The encrypted data is stored in the cloud. The Key Generation Center (KGC) generates the decryption key for data owner and sends it to the data owner.

3.3 Session Mediator (SEM) and Key Generation Center (KGC)

The users request to access the data from the cloud. If user is valid person, key generation center sends decrypt key to user at the same time it send decryption key information and data information to Session Mediator (SEM Keys). Session Mediator is responsible for maintaining the user session and provides the security on data. If user time limit exceeds session mediator close the connection of user session. The Session Mediator validates the decryption key session validity.

3.4 Data Access by user

The users request the cloud for accessing the stored data. In order to giving the request to the cloud the user need to register his/her name and password. After getting the decryption key by the KGC and validation by SEM the user can access the data from the cloud. Users can decrypt the data using the decryption key. Users can use the data depend on the type of data. Because session mediator gives the accessibility to users depend on the data.

References

1. Hameed Hussain, J., Sharavanan, R., Floor cleaning machine by remote control, AInternational Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-461-464, 2017
2. Hameed Hussain, J., Srinivasan, V., Extraction of polythene waste from domestic waste, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-427-431, 2017
3. Hameed Hussain, J., Thirumavalavan, S., Flow analysis of copper tube for solar trough collector without joint, International Journal of Pure and Applied Mathematics, V-116, I-14 Special Issue, PP-541-544, 2017
4. Hanirex, D.K., Kaliyamurthie, K.P., Mining the financial multi-relationship with accurate models, Middle - East Journal of Scientific Research, V-19, I-6, PP-795-798, 2014
5. Hemapriya, M., Meikandaan, T.P., Repair of damaged reinforced concrete beam by externally bonded with CFRP sheets, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-473-479, 2017
6. Hemapriya, M., Meikandaan, T.P., Experimental study on changes in properties of cement concrete using steel slag and fly ash, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-369-375, 2017
7. Hemapriya, M., Meikandaan, T.P., Experimental study on structural repair and strengthening of RC beams with FRP laminates, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-355-361, 2017
8. Hemapriya, M., Meikandaan, T.P., Effect of high range water reducers on sorptivity and water permeability of concrete, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-377-381, 2017
9. Hemapriya, M., Meikandaan, T.P., Strength and workability characteristics of super plasticized concrete, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-345-353, 2017
10. Hemapriya, M., Meikandaan, T.P., Potency and workability behavior of quality plasticized structural material, International Journal of Pure and Applied Mathematics, V-116, I-13 Special Issue, PP-363-367, 2017
11. Hussain, J.H., Manavalan, S., Optimization of properties of jatropha methyl Ester (JME) from jatropha oil, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-481-484, 2017
12. Hussain, J.H., Manavalan, S., Optimization and comparison of properties of neem and jatropha biodiesels, International Journal of Pure and Applied

- Mathematics, V-116, I-17 Special Issue, PP-79-82, 2017
13. Hussain, J.H., Meenakshi, C.M., Simulation and analysis of heavy vehicles composite leaf spring, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-135-140, 2017
 14. Hussain, J.H., Nimal, R.J.G.R., Review: Investigation on mechanical properties of different metal matrix composites in diffusion bonding method by using metal interlayers, International Journal of Pure and Applied Mathematics, V-116, I-18 Special Issue, PP-459-464, 2017
 15. Jagadeeswari, P., Subashini, G., Basic results of probability, International Journal of Pure and Applied Mathematics, V-116, I-17 Special Issue, PP-275-276, 2017
 16. Janani, V.D., Kavitha, S., Conceptual level similarity measure based review spam detection adversarial spam detection using the randomized hough transform-support vector machine, International Journal of Pure and Applied Mathematics, V-116, I-9 Special Issue, PP-197-201, 2017
 17. Jasmin, M., Beulah Hemalatha, S., Security for industrial communication system using encryption / decryption modules, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-563-567, 2017
 18. Jasmin, M., Beulah Hemalatha, S., VLSI-based frequency spectrum analyzer for low area chip design by using yasmirub method, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-557-560, 2017
 19. Jasmin, M., Beulah Hemalatha, S., RFID security and privacy enhancement, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-535-538, 2017
 20. Jasmin, M., Beulah Hemalatha, S., Digital phase locked loop, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-569-574, 2017
 21. Jeyalakshmi, G., Arulselvi, S., Community oriented configurations for WSN, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-529-533, 2017
 22. Jeyalakshmi, G., Arulselvi, S., Investigating file systems, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-517-521, 2017
 23. Jeyalakshmi, G., Arulselvi, S., Methodology for the development of lambda calculus, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-511-515, 2017
 24. Jeyalakshmi, G., Arulselvi, S., Remote procedure calls in access points, International Journal of Pure and Applied Mathematics, V-116, I-15 Special Issue, PP-523-526, 2017

25. Jeyanthi Rebecca, L., Anbuselvi, S., Sharmila, S., Medok, P., Sarkar, D., Effect of marine waste on plant growth, *Der Pharmacia Lettre*, V-7, I-10, PP-299-301, 2015
26. Kaliyamurthie, K.P., Parameswari, D., Udayakumar, R., Malicious packet loss during routing misbehavior-identification, *Middle - East Journal of Scientific Research*, V-20, I-11, PP-1413-1416, 2014
27. Kanagavalli, G., Sangeetha, M., Intelligent trafficlight system for reducedfuel consumption, *International Journal of Pure and Applied Mathematics*, V-116, I-15 Special Issue, PP-491-494, 2017
28. Kanagavalli, G., Sangeetha, M., GPS based blind pedestrian positioning and voice response system, *International Journal of Pure and Applied Mathematics*, V-116, I-15 Special Issue, PP-479-484, 2017
29. Kanagavalli, G., Sangeetha, M., Detection of retinal abnormality by contrast enhancement methodusing curvelet transform, *International Journal of Pure and Applied Mathematics*, V-116, I-15 Special Issue, PP-497-502, 2017
30. Kanagavalli, G., Sangeetha, M., Design of low power VLSI circuits for precharge logic, *International Journal of Pure and Applied Mathematics*, V-116, I-15 Special Issue, PP-505-509, 2017
31. Kanniga, E., Selvamarathnam, K., Sundararajan, M., Kandigital bike operating system, *Middle - East Journal of Scientific Research*, V-20, I-6, PP-685-688, 2014
32. Karthik, B., Arulselvi, Noise removal using mixtures of projected gaussian scale mixtures, *Middle - East Journal of Scientific Research*, V-20, I-12, PP-2335-2340, 2014
33. Karthik, B., Arulselvi, Selvaraj, A., Test data compression architecture for lowpower vlsi testing, *Middle - East Journal of Scientific Research*, V-20, I-12, PP-2331-2334, 2014
34. Karthikeyan, R., Michael, G., Kumaravel, A., A housing selection method for design, implementation&evaluation for web based recommended systems, *International Journal of Pure and Applied Mathematics*, V-116, I-8 Special Issue, PP-23-27, 2017
35. Khanaa, V., Thooyamani, K.P., Using lookup table circulating fluidised bed combustion boiler by the method of sensor output linearization, *Middle - East Journal of Scientific Research*, V-16, I-12, PP-1801-1806, 2013
36. Khanaa, V., Thooyamani, K.P., Face routing protocol using genetic algorithm in, *Middle - East Journal of Scientific Research*, V-16, I-12, PP-1863-1867, 2013
37. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Two factor authentication using mobile phones, *World Applied Sciences Journal*, V-29, I-14, PP-208-213, 2014
38. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Next major

- wave of it inovation, World Applied Sciences Journal, V-29, I-14, PP-218-220, 2014
39. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Traffic policing approach for wireless video conference traffic, World Applied Sciences Journal, V-29, I-14, PP-200-207, 2014
40. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Patient monitoring in gene ontology with words computing using SOM, World Applied Sciences Journal, V-29, I-14, PP-195-199, 2014
41. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Load balancing in structured PEER to PEER systems, World Applied Sciences Journal, V-29, I-14, PP-186-189, 2014
42. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Impact of route stability under random based mobility model in MANET, World Applied Sciences Journal, V-29, I-14, PP-274-278, 2014
43. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Modelling Cloud Storage, World Applied Sciences Journal, V-29, I-14, PP-190-194, 2014
44. Khanaa, V., Thooyamani, K.P., Udayakumar, R., Elliptic curve cryptography using in multicast network, World Applied Sciences Journal, V-29, I-14, PP-264-269, 2014
45. Khanaa, V., Thooyamani, K.P., Udayakumar, R., SRW/U as a lingua franca in managing the diversified information resources, World Applied Sciences Journal, V-29, I-14, PP-279-284, 2014

