www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Enhanced attribute-based data sharing key-exchange algorithm in cloud computing

E. Padma[1], G.Naveenkumar[2], R.Srinivasan[2], V.Yogesh[2], M.Vigneshwaran[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

[2]UG Students, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

ABSTRACT

Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a good technique for realizing fine grained data sharing, attribute-based encryption (ABE) has drawn wide attentions but most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. In this project, we present the comparison of Elgammal and pallier in term of encryption time, decryption time, throughput, encrypted file size and decrypted file size. In this paper, we use SHA-1 algorithm to evaluate performance by considering both encryption and decryption time.

General Terms: Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et.

Keywords: SHA-1, ABE, Elgammal, Pallier.

INTRODUCTION

Resource sharing in a pure plug and play model that dramatically simplifies infrastructure planning is the promise of cloud computing. The two key advantages of this model are ease of use and cost-effectiveness. Though there remain questions on aspects such as security and vendor lock-in, the benefits this model offers are many. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. This paper aims to provide a enhanced security for data sharing through cloud computing.

Cloud computing offers various services such as Software as a Service, Platform as a Service, Infrastructure. Not only it offers services it also different methods for cloud storage. The type of cloud storages are namely Private cloud, Public cloud, Hybrid cloud. Many organizations like Amazon provide public and private cloud services to the clients.

In this paper, we use Attribute-Based data sharing method using key exchange to share data over the cloud storages. The algorithms that are used in this paper are SHA-1, ABE (Attribute-Based Encryption), Elgammal and Pallier. SHA and ABE algorithms is used in key generation

Attribute-Based Encryption is a public key encryption in which both user's secret key and the ciphertext are attribute dependents. Attribute-based Encryption holds multiple keys which should only be able to access data if one individual key grants permission. Two types of attribute-based encryption Key-policy attribute-based encryption

Author for correspondence:
Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

and cipher text-policy attribute-based encryption. In this paper, ABE is used for the key generation and encryption process. ABE creates one symmetric in association with SHA-1.

The cryptographic hash function Secure Hash Algorithm 1(SHA 1) takes an input and creates a 160 bit message digest (which is a hexadecimal number and is 40 digits long). SHA 1 is considered as one of the prominent and most effective cryptographic hash functions which is used in key generation. With its powerful message digest value it provides almost effective way against an attack from the malicious node. In this paper, SHA 1(Secure Hash Algorithm 1) is used for the key generation along with attribute-based encryption method.

Elgammal encryption system is based on Diffie-Hellman key exchange which is an asymmetric key encryption algorithm for public key cryptography. The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. Elgammal is defined as a cyclic group and its security depends upon the difficulty of a certain problem related to computing discrete algorithms. In our paper, we have used this Elgammal encryption system to generate asymmetric keys.

METHODOLOGY

Along with Secure Hash Algorithm 1(SHA 1) two other methods also used for key exchange those are attribute-based encryption and Elgammal encryption systems. The basic principle of SHA-1 algorithm is that the plaintext data length is less than 2^ 64 bits and the output cipher text length is fixed for 256 bits. The SHA 1 algorithm needs the following resources:

ABE (Attribute Based Encryption)

Description

Sahai and Waters [2] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the ciphertext are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [3], ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CPABE) scheme. That can be discussed further.

ElGamalPaillier

Description

The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. It was described by Taher Elgamal in 1985. [1] ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is a variant of the ElGamal signature scheme, which should not be confused

with ElGamal encryption. ElGamal encryption can be defined over any cyclic group.

Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms The plain text is encrypted by the sender and then obtain the cipher text that is stored in cloud storage that is accessed by the cloud service provider. The cloud service performs the operations that user demands. It uses public key techniques to allow the exchange of private key encryption.

SHA-1

Description

In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

Since 2005 SHA-1 has not been considered secure against well-funded opponents, [4] and since 2010 many organizations have recommended its replacement by SHA-2 or SHA-3. Microsoft, Google, Apple and Mozilla have all announced that their respective browsers will stop accepting SHA-1 SSL certificates by 2017.

In 2017 CWI Amsterdam and Google announced they had performed a collision attack against SHA-1, publishing two dissimilar PDF files which produced the same SHA-1 hash.

SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD2, MD4 and MD5 message digest algorithms, but generates a larger hash value (160 bits vs. 128 bits).

SHA-1 was developed as part of the U.S. Government's Capstone project. The original specification of the algorithm was published in 1993 under the title Secure Hash Standard, FIPS PUB 180, by U.S. government standards agency NIST (National Institute of Standards and Technology). This version is now often named SHA-0. It was withdrawn by the NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly designated SHA-1. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function. According to the NSA, this was done to correct a flaw in the original algorithm which reduced its cryptographic security, but they did not provide any further explanation. Publicly available techniques did indeed demonstrate a compromise of SHA-0, in 2004, before SHA-1 in 2017.

SYSTEM ARCHITECTURE AND SECURITY MODEL

System architecture and design goals

As shown in Fig. 1, the system architecture of attribute based data sharing suitable for resource-constrained users in cloud computing consists of four entities AA (Attribute Authority).

CSP (Cloud Service Provider), MO (Mobile Data Owner), and DU (Data User). AA is a key entity who generates system public parameters and master keys. Especially, the system public parameters contain immediate cipher texts, which can be used by MO in the online phase. Also, AA manages users in the system and it's totally trustworthy by entities with in the attribute based data sharing system .MO may be a resource-constrained. entity WHO needs to soundly store a file on cloud storage servers maintained by CSP for sharing. Before it specifies the message, MO can generate offline cipher texts while accessing the power source. When the message becomes known, MO can calculate final cipher texts online without significantly draining the battery. CSP is guilty of saving the cipher text information of MO and it consists of a lot of cloud storage servers, which are maintained by a data service manager. DU is Associate in Nursing entity WHO contains a secret key and tends to access a cipher text hosted in CSP. In order to improve the efficiency of decryption, a public cipher text test phase is additionally introduced before the decryption phase. To be specific, after downloading the cipher text from CSP, DU should perform the test that if the cipher text is legitimate. And, the cryptography section is performed if and solely if the cipher text passes the test. In this work, it is assumed that all the entities except AA are

"honest-but-curious". More precisely, they will honestly execute the tasks assigned by legitimate parties but try to find out the maximum amount non-public data as doable. Data Confidentiality. Unauthorized users should be prevented from recovering the message of cipher texts. In addition, unauthorized access from CSP to the message of cipher texts should also be prevented.
Collusion-Resistance. Malicious users colluding with CSP should not reach decrypting the cipher text by combining their attributes if every of them cannot rewrite the cipher text alone. Also, the performance-related issue should be taken into consideration. Online/Offline Encryption. The scheme allows a resource constrained Mobile user to quickly transform a message into an ABE cipher text. Specifically, a lot of preparation work.Fig.one System design attributes based information sharing for resource-constrained users.

Computers & security be performed by alternative entities and also the mobile user whereas accessing power supply.

FIGURES

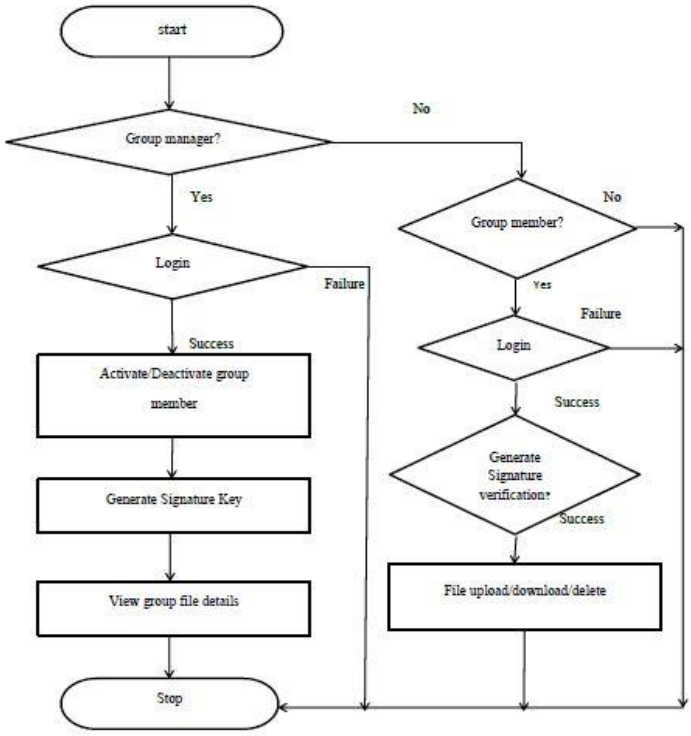

Fig.1-System architecture of attribute based data sharing for resource constrained users

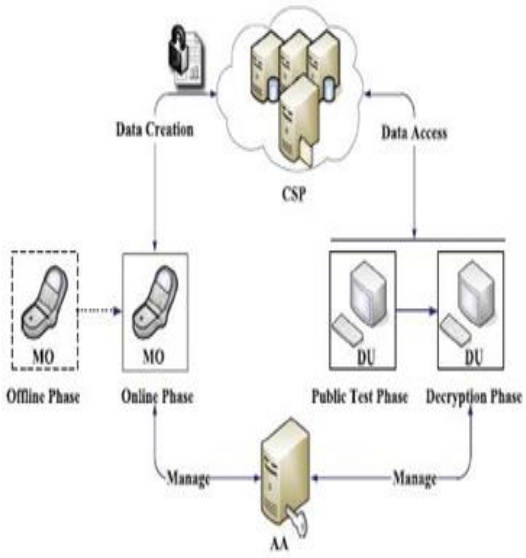

Fig.2-System Flow Diagram

Public Cipher text Test. Anyone can verify whether a cipher text is legitimate without requiring secret keys. Invalid cipher texts are thrown away without performing decryption. Based on the proposed system architecture, we define the attribute-based data sharing system suitable for resource on strained users in cloud computing. The system involves five phases as below.

Initialization

AA generates system public parameters and master keys for the system. All users can obtain the system public parameters, where immediate cipher texts are calculated by AA and employed in the following on-line information creation phase by MO.

User Registration

A user can join the attribute-based data sharing system by committing Associate in Nursing access structure to AA, who problems a secret key to the user supported the access structure.

Offline Data Creation

MO generates offline cipher texts, which are employed in the following online information creation section by MO. Online Data Creation. MO encrypts a file based on an attribute set and outsources the final cipher text to CSP for sharing. Data Access. DU downloads a cipher text from CSP. If the cipher text is legitimate, then MU decrypts it based on his/her secret keys.

CONCLUSIONS AND FUTURE WORK

Aiming at tackling the computation efficiency and weak data security issues in cloud data sharing, we propose an attribute based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme supports online/offline encryption modes and allows anyone to check the validity of cipher texts before high-priced full coding. Even the computation task in offline phase is significantly reduced by adding system public parameters. The proposed scheme is proven secure within the planned selective chosen attribute set and chosen cipher text security model under the wDBDH assumption. Theoretical analysis and experimental results indicate planned information sharing theme is extraordinarily appropriate for resource-limited mobile users. A attainable goal for our future analysis would be to think about direct attribute revocation in data sharing for resource limited users in cloud computing.

REFERENCES

[1]. AsmaJhari., Sonia Fernandes, "Techniques for Secure Multi - Owner Data Sharing in Cloud" ,International Journal of Engineering Science and Computing 2017.

[2]. EhabZaghloul, Kai Zhou and Jian Ren, "P-MOD: Secure Privilege Based Multilevel Organizational Data-Sharing in Cloud Computing" ,The authors are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing.

[3]. Fuchun Guo1, Yi Mu2, and Zhide Chen1, "Identity-Based Online/Offline Encryption", The authors are with the Department of Computer Engineering, Fujian Normal University, Fuzhou, China.

[4]. Guofeng Lin, Hanshu Hong and Zhixin Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", Citation information: DOI 10.1109/ACCESS.2017.2707126, IEEE Access.

[5]. HohenbergerS, Waters B. Online/offline attribute-based encryption. In: Public-key cryptography–PKC 2014. Springer 2014.

[6]. Jan Grashofer, Alexander Degitz and Oliver Raabe, "User-Centric Secure Data Sharing: Exploration of Concepts and Values", Maximilian Eibl, Martin Gaedke (Hrsg): INFORMATIK 2017, Lecture Notes in Informatics (LNI), GesellschaftfürInformatik 2017.

[7]. KaitaiLiang , Liming Fang, Duncan S, "A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds" Wiley Online Library 2014.

[8]. Li J, Li J, Chen X, Jia C, Lou W.Identity-based encryption with outsourced revocation in cloud computing. IEEE Trans Computer.

[9]. Li J, Jia C, Li J, Chen X. Outsourcing encryption of attribute-based encryption with map reduce. In: 14-th international conference on information and communications security (ICICS) 2012.

[10]. Li J, Huang X, Li J, Chen X, Xiang Y. Securely outsourcing attribute-based encryption with check ability. IEEE Trans Parallel DistribSyst 25(8), 2014, 2201–10. doi:10.1109/TPDS.2013.271

[11]. Melissa Chase," Multi-authority Attribute Based Encryption", The author is from Computer Science Department, Brown University, Providence, RI 02912

[12]. Madhubabu B N V and Dr Rajasekhararao K, "An enhanced attribute based encryption model using quantum key distribution for information security in cloud environment", International Journal of Advance Engineering and Research Development, 4, 2017.

[13]. Wang C, RenK,Wang J. Secure and practical outsourcing of linear programming in cloud computing. In: IEEE international conference on computer communications (INFOCOM). 2011.

[14]. Yang, "Hidden Policy Attribute -Based Data Sharing with Direct Revocation and Keyword Search in Cloud Computing 2018.

[15]. Zhang Y, Chen X, Li J, Wong DS, Li H. Anonymous attribute-based encryption supporting efficient decryption test. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.