ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Detecting malicious node attacks on WSN using ABE

M.Parvathi[1], K.Gokulchander[2], K.Karthikeyan[2], P.Mathivanan[2], G.Mohanram[2]

[1]Associate Professor

[2]UG Students

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 Elgamal 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, etc..,

Keywords: SHA-1, ABE, Elgamal, 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), Elgamal 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 cipher text 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 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.

Elgamal 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. Elgamal 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 Elgamal 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 Elgamal encryption systems.

The basic principle of SHA-1 algorithm is that the plaintext data length is less than 2^ 64 bits and the output ciphertext length is fixed for 256 bits.
The SHA 1 algorithm needs the following resources:

ABE (Attribute Based Encryption)

Description

Sahai and Waters 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 cipher text 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, 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.

ELGAMAL PAILLIER

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 Tahir Elgamal in 1985. 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, and since 2010 many organizations have recommended its replacement by SHA-2 or SHA3 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.

CONCLUSIONS

The proposed scheme supports online/offline encryption modes and allows anyone to check the validity of cipher texts before expensive full decryption. The proposed scheme is proven secure in the proposed selective chosen attribute set and chosen cipher text security model under the WDBDH assumption. A possible goal for our future research would be to consider direct attribute revocation in data sharing for resource limited users in cloud computing.

REFERENCES

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

[2]. Axin, Dong Zheng Yinghui Zhang ID and Menglei Yang, “Hidden Policy Attribute -Based Data Sharing with Direct Revocation and Keyword Search in Cloud Computing” 2018.

[3]. Ehab Zaghloul, 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.

[4]. 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.

[5]. Guofeng Lin, Hanshu Hong and Zhixin Sun, “A Collaborative Key Management Protocol inCiphertext Policy Attribute Based Encryption for Cloud Data Sharing”, Citation information: DOI 10.1109/ACCESS.2017.2707126, IEEE Access.

[6]. Jan Grashöfer, 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), Gesellschaft für Informatik. 2017.

[7]. Kaitai Liang , Liming Fang, Duncan S, “A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds” iley Online Library. 2014.

[8]. Madhu babu B N V and Dr Rajasekhara rao 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(11). 2017.

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

[10]. Mohay, "Mining email content for author identification forensics," ACM Sigmod Record, 30(4), 55-64, 2001.

[11]. Narayanan and V. Shmatikov, "De-anonymizing social net-works," Proc. Of the 30th IEEE Symposium on Security and Privacy (SSP'09), 2009, 173-187.

[12]. S. Bartunov, A. Korshunov, S. Park, W. Ryu, and H. Lee, "Joint link-attribute user identity resolution in online social net-works," The 6th SNA-KDD Workshop '12, 2012.