ISSN 2395-1621

Security Analysis On Re-Encryption Based Cloud Data

[#1]Rohini G. Dhope, [#2]Renuka S.Pandharkar, [#3]Ranjeet C. Hole, [#4]Anjali B. Pandhare, [#5]Asst Prof.Piyush P.Gawali

[1]rohinidhope31@gmail.com
[2]renu.pandharkar@gmail.com
[3]holeranjeet3800@gmail.com
[4]anjalipadhare99@gmail.com
[5]piyush.gawali@sinhgad.edu

[#12345]Department of IT
NBN Sinhgad Technical Institutes Campus Ambegaon(BK),Pune

ABSTRACT

Cloud computing is basically an Internet-based network made up of large numbers of servers - mostly based on open standards, modular and inexpensive. Clouds contain vast amounts of information and provide a variety of services to large numbers of people. The benefits of cloud computing are Reduced Service Leakage, Decrease evidence acquisition time, they eliminate or reduce service downtime, they Forensic readiness, they Decrease evidence transfer time the main factor to be discussed is security of cloud computing, which is a risk factor involved in major computing fields. We aim to achieve to highest security for Service on clouds, the application will be java-based application in which we will be working on 4 modules entry login, star marking and sms alert, cryptographic encryption and Image Steganography. This will benefit the security in clouds computing, as user Service will be approximately 100% secure, as this technique has cryptographic encryption as well as Image steganography encryption too. Advance Service theft detection and prevention is what we want to achieve.

Keyword: Cloud computing security, Data Sharing, Attribute based encryption, Theft-of-service Attack.

ARTICLE INFO

Article History

Received: 9th May 2018

Received in revised form :

9th May 2018

Accepted: 13th May 2018

Published online :

16th May 2018

I. INTRODUCTION

With the advent of cloud computing technology, data sharing via the Internet has become more economical and convenient than ever. While people are enjoying the convenience which cloud computing brings about, they are also facing with urgent data security issues. These issues arise from the fact that most cloud computing servers are operated by commercial providers which are very likely to be outside of the trusted domain of data owners. Thus, it is of great significance for users to take effective measures to protect the privacy of their data stored in the cloud.

Attribute based encryption (ABE) has been developed as a cryptographic primitive for the provision of fine-grained access control to the encrypted data and is especially suitable for data protection in cloud computing. In ABE, a user's access privileges are described by an access structure consists of several attributes and logical gates. A data owner can make self-centric access policies over the file to be encrypted, thus data sharing can be more expressive and flexible through ABE.

Later, the notion of attribute based proxy re-encryption (AB-PRE) have been proposed. In ABPRE, the original ciphertexts are encrypted over the delegator's 'attributes. However, if a delegator wants to share the original ciphertexts with some other de legatees, he can generate a re-encryption key. By using the re-encryption key, a semi-trusted server can transform the original ciphertexts into proxy ciphertexts which are encrypted by the delegatees' attributes, so any eligible delegatee can obtain the plaintext using the private key he possesses. During the whole process of proxy re-encryption, the server knows nothing about the plaintext, consequently, ABPRE is very suitable for data sharing in semi-trusted servers such as cloud computing.

However, ABPRE will prevent some common operation on ciphertexts, especially in terms of ciphertext searching. Since data are encrypted in the cloud server and the volume of data is large, it is inconvenient for a delegatee to fmd out

the desired files and contents hidden in the ciphertexts. One solution is the delegatee decrypts all the possible ciphertexts and search the desired file according to the plaintexts, but this will add considerable computation burden during decryption. Thus, a scheme which supports both the function of proxy re-encryption and ciphertext keyword search is urgently to be proposed.

In this paper, we present an attribute based proxy re-encryption scheme with keyword search (ABPRE-KS) to provide flexible and secure data sharing among users in the cloud. In our scheme, a user's access privileges are described by an access structure consisting of several attributes while ciphertexts are labeled by several target attributes. A delegator can transform the original ciphertexts into proxy ciphertexts encrypted by the delegatee's attributes without leaking any sensitive information to the cloud server. Moreover, our scheme allows a delegator to generate search indexes on the keywords related to ciphertexts. If a delegatee's credentials satisfy the delegatee's access policy, then the delegatee can search his desired files at a fast rate without decrypting the possible ciphertexts. By security analysis, our ABPRE-KS is confidential and keyword semantic secure under BDBH assumption.

II. LITERATURE SURVEY

The 2014"Survey on Fog Computing Mitigating Data Theft Attack in Cloud". Thus in this paper we propose a distinct technology to make the cloud safer by securing the personal and the important data of the business firms. We provide monitoring of the access to the account by checking the behavior of the user. We provide access not only by login credentials but also by challenge questions which would be only know to the user. If access found to be unauthorized thus providing with the fake data so that the real data of the user can be saved. This technology would app up a level in securing the data on the cloud.

The 2016 year "Improve Lightweight Proxy Re-Encryption For Flexible and Scalable Mobile Revocation Management in Cloud Computing". We have proposed a VL-PRE which is a proxy-based re-encryption scheme as an improvement over our previous work on PRE. This new approach explaits a reduction of the size of root decryption key and relies on key updates instead of key generations. These two contribution over the previous work create a new scheme that requires less memory and less computation. Therefore, it is possible for data owners to support secure attribute revocation or policy update through resource constrained devices.

The 2017 year "Enhancing Image Security and Privacy in Cloud System Using Steganography". In this paper, an image protection method is proposed to ensure digital image security and privacy over the cloud system. We use the Steganography technique to camouflage the luminance as well as the subsampled chroma components of a private image. As shown in the experiments, the proposed method can conceal any a private color image. Illegal hackers and attakers will not perceive the existence of private image even they intruded lawlessly into the cloud storage. Moreover, the proposed method can reduce the size of the image file and increase the cloud capacity.

The 2017 year "Towards Secure Data Sharing in Cloud Computing using Attribute Based Proxy Re-Encryption with Keyword Search ". In this paper, We present an attribute based proxy re-encryption scheme with keyword search(ABPRE-KS).Which combined the merits of attribute based re-encryption and keyword search we present the concrete algorithm of our scheme and construct the security model under DBDH hardness assumption. The proposed ABPRE-KS support flexible and secure data access control among user and it is very sutiable for providing big data secure sharing in Cloud enviorments.

The 2016 year "An Identification and Preventi on of Theft-of-Service Attack on Cloud Computing" He success rate of cloud computing is directly proportional to the rate of attacks against it. Cloud service provider must provide security to cloud architecture so user can avail the wide variety of benefits. Theft-of-service attack tar gets the cloud infrastructure and uses the malicious VM for hostile actions.

The 2016 year "Detection and Response of Identity Theft Within a Company Utilizing Location Information" Extracting data after comparing the physical location and system login time is very suggestive. The dangerous factors can be summarized only by grasp of the current state of identity theft which happens in the company. Establishment of security policy, improvement of employee's security consciousness, and security education can be accomplished based on the real cases.

The 2017 year "Identity Theft Detection in Mobile Social Networks Using Behavioral Semantics" In this work, we apply state-of-the-art methods to a clas-sical problem, identity theft detection. Firstly, we find that semantic features achieve better performance than spatial features. Secondly, we find different types of features have a complementary effect in identity theft detection. Finally, our detection based on the joint model is interpretable since we can get the conditional probability in each dimension to support our judgment.

III. ARCHITECTURE

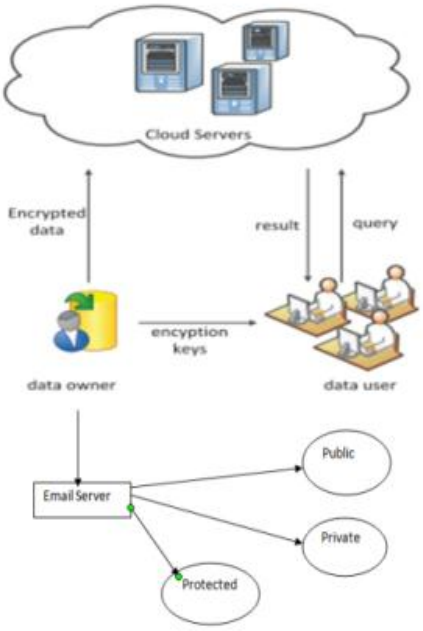

Fig 1.Architecture

IV. RELATED WORK

1. RSA ALGORITHM

RSA Algorithm is most commonly used to encrypt and to authenticate. It has been also used as web browser from Microsoft and Netscape. RSA uses public key cryptography, it involves private key and public key. The public key is used to encrypt the message and can be know to everybody RAS algorithm involves three main steps key Generation, Encryption, Decryption.

In this algorithm two large prime numbers are multiplied with additional operations results into a set of two numbers Which contains a public key and other set contains a private key. Public and Private keys required to encrypt and decrypt with only the owner should know it.In this algorithm private key is not sent decrypt the text that has been previously encrypted by a public key.

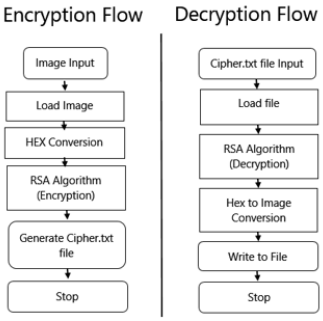

Fig.2. RSA Algorithm Flow Chart

KEY GENERATION

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purpose the integers p and q should be chosen at random and should be similar in magnitude but differ in length by a few digits to make factoring harder.prime integers can be efficiently found using primality test .
2. Compute n=pq
   - n is used as the modulus for both the public and private keys its length,usually expressed in bits,the key length.
3. Compute λ(n)=lcm(λ(p),λ(q))=lcm(p-1,q-1),Where λ is Carmichael's totient function.This value is ket private.
4. Choose an integer e such that 1<e<λ(n) and gcd(e,λ(n))=1 i.e e and λ(n) are coprime.
5. Determine d as d=e^{-1}(modλ(n));i.e d is the modular multiplicative inverse of e(modula λ(n)).
   - This is more clearly stated as: solve for d given d.e≡1(modλ(n)).
   - E having a short bit-length and small Hamming weight results in more efficient encryption-mostly commonly e=$2^{16}+1$=65,537.However,much smaller values of e have been shown to be less secure in some settings.
   - e is released as the public key exponent.
   - d is kept as the private key exponent.

ENCRYPTION

After Bob obtains Alice's Public key,he can send a message M to Alice.To do it,be first turns M into an integer m,such that 0≤m<n by using an agreed-upto reversible protocol know as a padding scheme. He then computes the cipertext C using Alice's public key e corresponding to c≡m^e(mod n) This can be done reasonably quickly,even for 500-bit numbers, using modular exponentiation.Bob the transmits c to Alice.

DECRYPTION

Alice can recover m from c by using her private key exponent d by computing

c^d≡(m^e)≡m(mod n)

Given m,she can recover the original message M by resersing the padding scheme.

2. STEGANOGRAPHY

A Steganograhy System is quintuple p=(C,M,K,D_K,E_K),Where C is the set of all cover used in communication M is the set of all secret messages that need to be transported using the covers, K the set of secret keys. E_K:C X M X K→C, and D_k:C X K→M two functions,the embedding and the extraction fuctions respectively such that:$D_k(E_K(c,m,k))$=m.

Note that in the definition above no care is taken in what concerns the means by which Alice and Bob handle the key exchange under the assumption of an existing shared secret key between the two parties.the framework dicussed above is named secret Steganography.Its counterpart Public key steganography is based on the same principle as public key cryptography.Another category of setganography pure steganography does not assume the existence of a shared secret between the two parties:In fact the effectiveness of pure steg-system lies in secrecy of the two embedding functions.thus violating kerchoff principles the security of the system should only depend on the secrecy of the key and not on that of the algorithm.

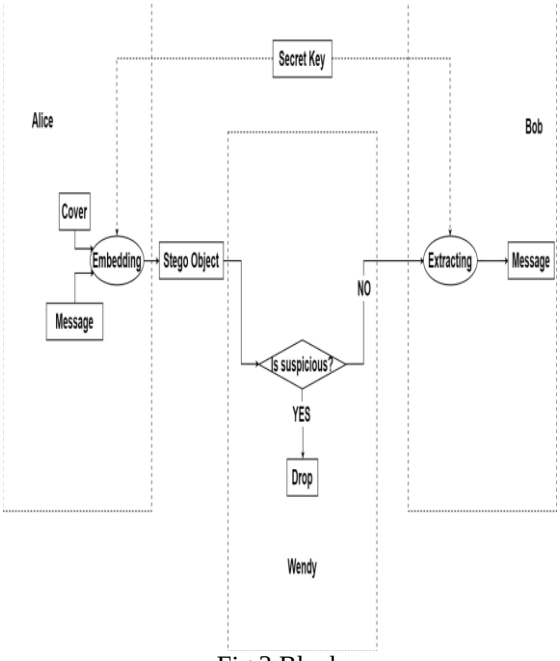

Fig.3.Block

V. CONCLUSION

We proposed Advance Service theft detection and prevention system (ADTDAP), which will provide approximately 100% security to the Service on cloud computing. The approach is java based application based on AES and OTP algorithm, the cryptographic encryption and image steganography is being used in order to provide security to the Service on cloud.

REFERENCE

1. Viraj G. Mandlekar,Vireshkumar Mahale,Sanket S.Sancheti,Maaz S.Rais"Survey on for Computing Mitigating Data Theft Attacks in Cloud"International Journal of Innovative Research in Computer Science and Technology (IJRCST) ISSN:2347-5552,Volume-2,Issue 6,November-2014.

2. Hanshu Hong,Zhixin Sun*"Towards Secure Data Sharing in Cloud Computing Using Attribute Based Proxy Re-Encryption with Keyword Search"2017 the 2^{nd} IEEE International Conference on Cloud Computing and Big Data Analysis.

3. Somchart Fugkeaw,Hiroyuki Sato"Improved LightWeight Proxy Re-Encryption For Flexible and Scalable Mobile Revocation Management in Cloud Computing"2016 IEEE 9^{th} International Conference on Cloud Computing.

4. Ms.M.Malthi,Mr.M.Rahul,Mr.N.SathishKumar,Mr.R.Thamaraiselvan "Enhanced Image Steganography Using AES and SPIHT Compression"2017 International Conference on Innovations in Information Embedded and Communication System(ICIIECS).

5. Tarun Jain,Anita Shrotriya,Vivek Kumar Verma,horesh Kumar" Mask Encryption Based Highly Secure Image Steganography".2017 International Conference on Intelligent Communication and Computational Techniques(ICCT) manipal University Jaipur,Dec 22-23,2017.

6. Wen-Chuan Wu and Shang-Chian Yang"Enhancing Image Security and Privacy in Cloud System Using Steganography"2017 IEEE International Conference on Consumer Electronics-Taiwan(ICCE-TW).

