P.Ananthi *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 12, December- 2016, pg. 21-27 **ISSN: 2321-8363**
Impact Factor: 4.123

Encryption Based Security Model for Cloud Environment

P.Ananthi[1], G.R.Sreekanth[2]

[1] Assistant Professor, Kongu Engineering college, India, ananthiparth@gmail.com

[2]G.R.Sreekanth, Assistant Professor, Kongu Engineering college, India, grsreekanth@kongu.ac.in

Abstract

In recent day, the enormous usage of cloud services leads to much concerned on cloud security. This paper primarily considers the important aspect of cloud security based on encryption. The users perform secure search on cloud environment using this method. Data stored in cloud are encrypted which ensure the privacy of the user; the files are encrypted before uploading. At the time of searching the file user can provide keywords to search on encrypted data. This encryption scheme based on two types symmetric key and asymmetric key. The first model is using users own secret key to encrypt the file and upload that. The second model is used for file sharing user use public key of receiver. The receiver then uses his private key to search the data.

Keywords: Cloud Security, Public Key Encryption, Symmetric Key encryption

1. Introduction

Cloud computing has gained wide acceptance for organizations as well as individuals by introducing computation, storage and software based services. It is used to address the resource scarcity issues of its clients by providing them with on-demand pay-per-use services incorporates a centralized collection of resources called a cloud connected through a high speed network. The global availability of high performance resources, support of a large number of services, and ability to store large amount of data have made it ubiquitous. Even with the modern smartphones, the cloud computing is able to serve multiple purposes ranging from backup of contacts to the execution of complex applications through computation offloading. Moreover, the reduced cost of services and an assurance regarding quality make it an attractive solution for mitigating the issue of constrained resources. Since a cloud computing platform provides services by sharing valuable resources, an adequate usage of these resources may be achieved by ensuring that the platform is able to counter security threats which may otherwise deteriorate its performance and reliability.

With the rapid development of information technology, the data of the Internet is an explosive growth. The emergence of Cloud Computing [1–3] turns to be a promising paradigm for massive data storage, more

specially, cloud Storage service. Cloud computing has been the hottest word in the IT area. It provides services in a pay-per-use model to users who can access the network. Similarly cloud storage provides users on-demand storage service, such as Dropbox, Amazon Simple Storage Services (S3), and Google Drive. Using these services, users can upload their data to the cloud storage server, and access their online data over the network regardless of when and where they are. For business users, rather than building their own data center, the company can leverage cloud storage service to store their data to the cloud storage server. As shown above, cloud services provided us very huge convenience. However, the security of the cloud is far from satisfying. Cloud security [4,5] has become a challenging problem towards data of users and companies when they adopt cloud services.

Cloud security can be classified into storage security and computation security [6]. Storage security means the users' data privacy of online storage, such as avoiding data leakage, data integrity, and assured data deletion. Since in cloud services data is stored online, data owners lost the ultimate control of their data, then they cannot physically protect data from attackers' interception or manipulation. For cloud computation aspect, when users delegate the cloud server to do some computation, such as keyword search and scientific computation, cloud may not perform a secure and exact computation for the sake of saving computing resources, hence users also need to guarantee data privacy during cloud computation.

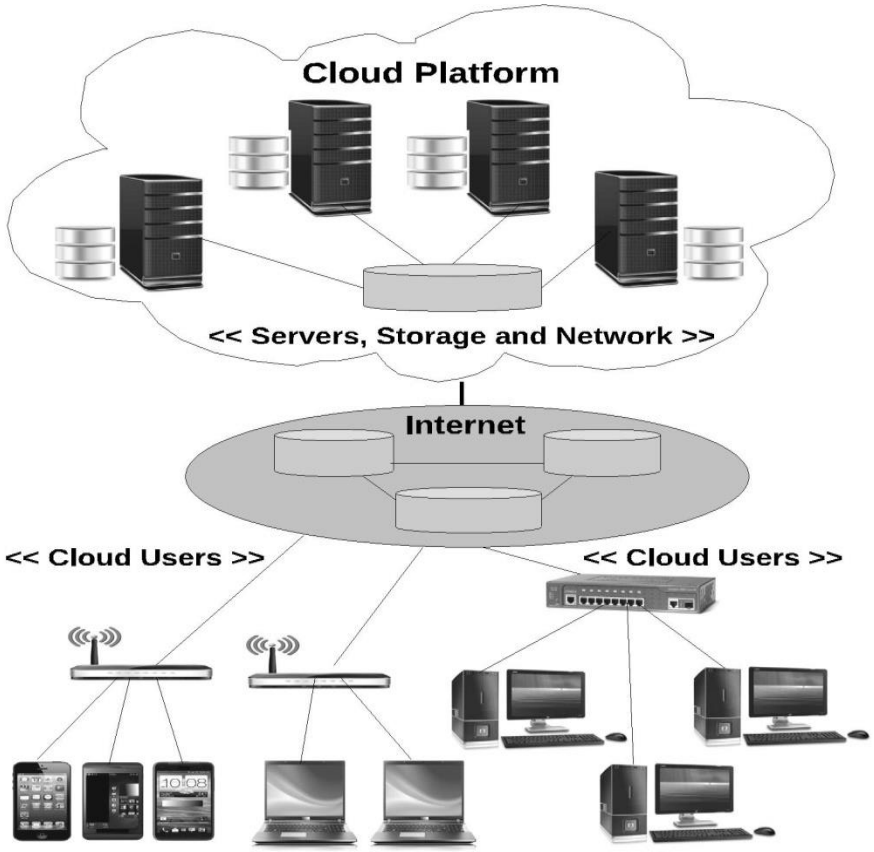

Figure. 1 Public cloud computing platform

An overview of a public cloud computing platform is shown in Fig. 1. The cloud platform is usually equipped with high performance server machines, high speed storage devices and an efficient network. The cloud users having mobile phones, laptops or modern desktops connect to the cloud platform through internet. Since the server machines are connected using an internal network, an attack on the network may produce a detrimental impact in the form of communication delays or even the network being inaccessible. Likewise, the attacks on virtual machines and hypervisors being used to run virtual machines have shown to severely breach the security for malicious purposes. Similarly, the cloud services are also prone to security threats as this layer contains software which has always been vulnerable to hacks and security attacks. These attacks may cause violation of data protection or even unavailability of services for all the clients.

This paper provides a systematic survey on encryption in three aspects such as security requirements of cloud environment, searching methodology and deployment model hunting encryption is an encryption system that supports keyword search. The rest of this paper is organized as follows. In Section 2, various security issues are addressed. The proposed methodology is present in Section 3. In Section 5, will give conclusion and future scope of research.

2. Security Issues

Data breaches: Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating.

Compromised credentials and broken authentication: Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user's job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization.

Hacked interfaces and APIs: The security and availability of cloud services -- from authentication and access control to encryption and activity monitoring -- depend on the security of the API. Risk increases with third parties that rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials, the CSA warned. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.

Exploited system vulnerabilities: System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces.

Account hijacking: Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks.

Malicious insiders:T he insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business partner. The malicious agenda ranges from data theft to revenge. In a cloud scenario, a hellbent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

DoS attacks: DoS attacks have been around for years, but they've gained prominence again thanks to cloud computing because they often affect availability. DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. While high-volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities.

Shared technology, shared dangers: Vulnerabilities in shared technology pose a significant threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone. "A single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud," the report said.

3. Proposed Methodology

This encryption consists of three parties, a cloud storage server, data owners and receivers. The cloud storage server is the party that stores the data uploaded by data owner executes the test algorithm, and then return the result to receivers. Data owners is the party that owns the data files and encrypts them before uploading. Receiver is the party who want to execute some keyword search and get the result. The framework can be concluded as followed:

A) Data owner encrypts his data files and the associated keywords index, then uploads encrypted files to storage server.
B) If a receiver wants to issue a keyword search, he first computes the trapdoor responding to the keyword and sends this trapdoor to server.
C) When server gets the search request, he computes the trapdoor with encrypted index to find if there exists some match. If so, send the data files which contain this keyword to the receiver.

3.1 Framework of searchable encryption

A general searchable encryption scheme consists of four algorithms:

Algorithm 1: The setup algorithm takes as inputs a security parameter and then it outputs the keys of the scheme.

Algorithm 2: The encryption algorithm takes as inputs the data files collection along with keys generated above, encrypts the data files and associated keywords index.

Algorithm 3: The trapdoor algorithm takes as inputs the target keyword and secret key. It generates the trapdoor by encrypting keyword with secret key.

Algorithm 4: The test algorithm takes as inputs the encrypted keyword index and trapdoor of target keyword, by computing it returns 1 if success, otherwise return 0.

Users and storage server can apply the above four algorithms to complete the search. The Setup algorithm generates keys for running whole encryption system. The user generates associated keywords index for data files, and encrypts index by running Enc algorithm. Then user uploads the ciphertext and secure index to the storage server. The receiver picks a target keyword and generate trapdoor for this keyword by running Trapdoor algorithm, then sends it to the server. As the server receives the search query, it runs Test algorithm with encrypted index and trapdoor. If success, then return the files associated with the matching keyword.

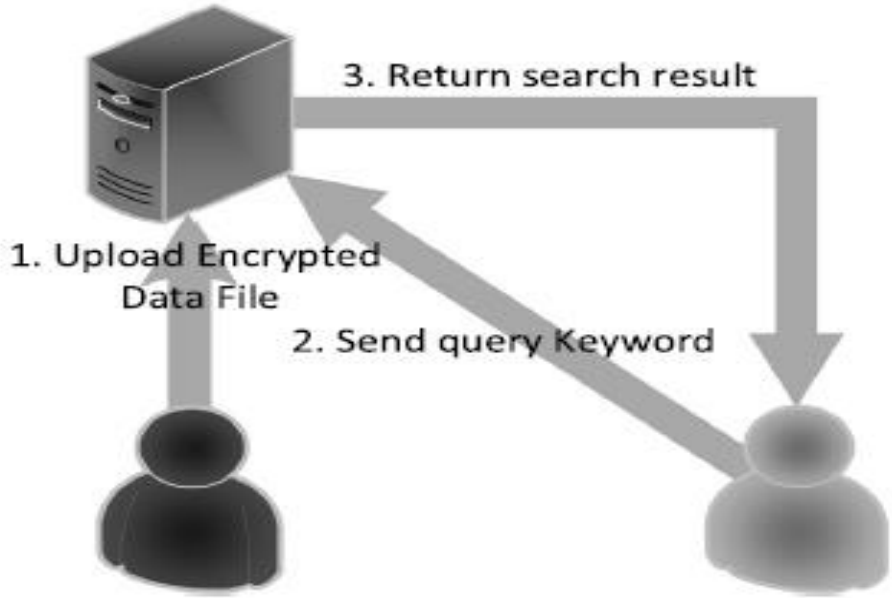

Figure.2 Uploading and Downloading Encrypted File

A PEKS scheme consists of four algorithm, KeyGen, PEKS, Trapdoor, Test. KeyGen algorithm generated the public key/secret key pair. In PEKS algorithm, user encrypted the keywords of data files with public key and attached it to the data files. Trapdoor algorithm takes the secret key and target keyword as input and output the trapdoor of target keyword. Finally server run Test algorithm and get the search result. The processing of scheme is depicted in Figure. 3.

This scheme is a pioneer construction for public key based encryption. However it exists some problems. First, the construction is oriented to mail system, so the sender can be multi-users, but it should only assign a single user to decrypt it in advance. This may not be appropriate in some other application scenarios. Second, the construction need a secure channel between server and receiver (User B) to guarantee the privacy. Involving in a secure channel makes the scheme very inefficient and impractical. Third, the construction only support single keyword search. In Trapdoor algorithm, receiver can only generate trapdoor for single keyword. This is also not practical in real applications. The main idea is the trapdoor of some keyword is only valid in some specific time period. Server cannot search on later or future ciphertexts with this trapdoor.

There are other construction for different application scenarios in [7], such as public key encryption with registered keyword search (PERKS), public key encryption with delegated search (PEDKS) etc. The main idea is that it only allows data owners to build trapdoors for the keyword which have been previously registered by searchers. This construction can efficient resist keyword guessing attack. PEDKS scheme used ElGamal Cryptosystem to allow server to search on each part of the data ciphertext, other than only to search on the metadata part. Researchers also used proxy re-encryption (PRE) scheme to construct PRE-based searchable encryption.

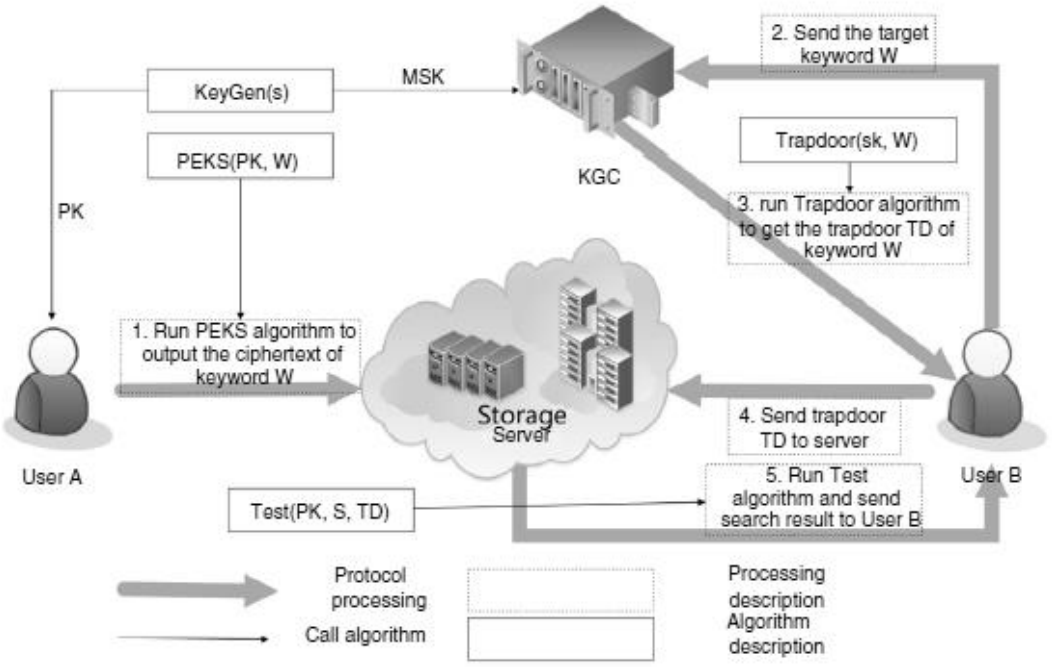

Figure.3 PEKS Scheme Model

4. Conclusion

Cloud security has turned to be a main concern about the deployment of cloud computing. This article presented an overview about searchable encryption, which is an important challenging problem in cloud security. Firstly presented the security issues and search functionality of searchable encryption. Then discussed deployment model with encryption according to application scenarios. The existing works are mainly concern with security, efficiency and expressiveness. As mentioned above, searchable encryption can be an efficient and secure solution to private database retrieval. Meanwhile, it is not so mature, so it needs to be deeply studied to fully implement to cloud computing. Eventually searchable encryption will provide users to privately search on database stored in cloud storage, and privacy of users and cloud servers will be well protected.

References

[1] P. Mell, T. Grance, The NIST definition of cloud computing. NIST Special publication. 2011. [Online] Available: http://predeveloper.att.com/home/learn/enablingtechnologies/ The_NIST_ Definition_of_ Cloud_ Computing.pdf.

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing, Commun. ACM 53 (4) (2010) 50–58.

[3] D. Feng, M. Zhang, Y. Zhang, Z. Xu, Study on cloud comput-ing security, Ruan Jian Xue Bao/J. Softw. 22 (1) (2011) 71–83. http://dx.doi.org/10.3724/SP.J.1001.2011.03958. (in Chinese with English abstract) http://www.jos.org.cn/1000-9825/3958.htm.

[4] S. Kamara, K. Lauter, Cryptographic cloud storage, in: Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2010, pp. 136–149.

[5] H. Takabi, J.B.D. Joshi, G.J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. 8 (6) (2010) 24–31.

[6] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.
[7] M. Abdalla, M. Bellare, D. Catalano, M. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi, Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions, in: Advances in Cryptology, CRYPTO 2005, Springer, Berlin, Heidelberg, 2005, pp. 205–222.
[8] C. Liu, L. Zhu, M. Wang, Y.A. Tan, Search pattern leakage in searchable encryption: Attacks and new construction, Inform. Sci. 265 (2014) 176–188.
[9] O. Goldreich, Foundations of Cryptography: Volume 2, Basic Applications, Cambridge University Press, 2009.
[10] J. Baek, R. Safavi-Naini, W. Susilo, Public key encryption with keyword search revisited, in: Computational Science and Its Applications, ICCSA 2008, Springer, Berlin, Heidelberg, 2008, pp. 1249–1259.
[11] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: Advances in Cryptology, Eurocrypt 2004, Springer, Berlin, Heidelberg, 2004, pp. 506–522.
[12] L. Fang, W. Susilo, C. Ge, J. Wang, A secure channel free public key encryption with keyword search scheme without random oracle, in: Cryptology and Network Security, Springer, Berlin, Heidelberg, 2009, pp. 248–258.
[13] L. Fang, W. Susilo, C. Ge, J. Wang, Public key encryption with keyword search secure against keyword guessing attacks without random oracle, Inform. Sci. 238 (2013) 221–241.
[14] H.S. Rhee, J.H. Park, W. Susilo, D.H. Lee, Trapdoor security in a searchable public-key encryption scheme with a designated tester, J. Syst. Softw. 83 (5) (2010) 763–771.

A Brief Author Biography

[1]**Dr.P.Ananthi** (Ananthi Pazhanisami) obtained the MSc degree in the year 1999 and completed M Phil degree in the year 2004 in Bharathiar University, Coimbatore. She received PhD degree from Anna university, Chennai in 2015 in the field of Network Security. She has 17 years of experience in Engineering Colleges. She is working as Assistant professor in the Department of Computer Technology, Kongu Engineering College, India. She has published 10 research articles in reputed international journals. She has organized many seminars/workshops/SDPs/STTPs Sponsored by number of funding agencies for the benefit of faculty members and research scholars. Her specialization includes Network Security, Fuzzy Neural Network, Data mining.

[2]**G.R.Sreekanth**, obtained ME degree in the year 2007 and doing doctorate in the area of MANET in Anna university, Chennai. He is working as Assistant Professor in department of CSE, Kongu Engineering College and he has 17 yrs UG& PG teaching experience. He has published 6 papers in International Journals and 15 papers in National and International Conferences. His area of interests are Ad hoc networks, databases and Software Engineering.

