IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 2 - V7I2-1479)
Available online at: https://www.ijariit.com

Public key encryption with keyword search

Lokeswary Sridhar
ls4998@srmist.edu.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Shyam Sundar N.
sn3596@srmist.edu.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Sujith K.
su5015@srmist.edu.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Dr. Durga Devi P.
durgadep@srmist.edu.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

Today's entrepreneured world demands huge storage for the data and elementary sharing of the same. Cloud storage serves the requirement of providing security to the files uploaded by the organizations. Security prior to uploading the data is provided by encrypting the files and creating keywords to shield the organizational secrets from strangers. The other challenge faced by the organizations is the Insider keyword guessing attack, which results in the hackers being the employees themselves.To address this variant of threat, We propose a system that has a hierarchy developed between the employees such that the higher-level employees can monitor the activities of the lower-level workforce by constructing a semi-generic Public Key Tree. The PK-tree is constructed by the support provided by the Hierarchical Public Key Encryption with Keyword search [HPEKS] a variant of the public key encryption with keyword search [PEKS]. It furthermore enjoys transparency to the owner provided the admin-1 verifies the user login and Admin-2 will send the OTP (One time Password) such as the secret key to the user to their Registered mail Id which will be used to secure the data and records the activity. The efficiency of the system is analyzed by eradicating the insider attack threat.

Keywords: *Hierarchical, Public-Key, Encryption, Keyword-Search, Cloud, Storage, Database, Secured-Data, Insider, Keyword, Guessing-Attack, Admin, User, Owner, Security Purpose*

1. INTRODUCTION

Data Integrity is the most alarming consideration for the structure.Losing files entails a loss of both time and resources to recover and restore the data essential for the business. Data integrity happens due to many reasons such as human errors, virus attacks, computer theft, disasters, hackers and insiders[1], etc.Human errors are infallible, they are very common to happen which may result in a huge flaw that cannot be resolved. This error can also serve as a model for the errors such as software corrupt, liquid spill, hard drive formatting. On the other hand, viruses can steal or delete huge amounts of data and can bring all the business operations to fall. Computer theft can happen anywhere when it is left unattended [2].

Human attackers such as hackers and insiders can not just steal the data but also can destroy the entire computing system causing a huge loss for the organization. This can happen through various modes few of which are using a weak network, usage of a system that is poorly secured, lack of monitoring or even usage of passwords that are easy enough to guess and crack open the file.The undeniable truth is that the hackers sometimes are the employees of the organization or the network provider themselves. Hacking happens when the data is stored in the most vulnerable format or lacks the monitoring required. Security for the data stored is a must but also must be stored in the most secure way.Cloud storage is the most effective way of backing up or storing data. It can be accessed easily and is also secured. But the data is again vulnerable in this stage also[3]. To prevent that there are ways to encrypt the files and access them, but it cannot prevent the insider attacks. Thus, the Public key encryption with watch word search helps in introducing the monitoring system, where the owner of the files can monitor the access of the.employees[4]. Thus, in the proposed system we have introduced the PK-Tree which inculcates the monitoring method in the system, preventing the insider attack.

2. LITERATURE SURVEY

Yu Zhang, Yifan Wan, Yin Li[6] have used the Searchable.public.key encryption (SPE) is a form of public key encryption that facilitates multi-keyword searches and enables users of data to quickly retrieve files that have been locked of their choice. It has received a lot of attention in recent years. Most current Search Public Encryption (SPE) solutions, on the other hand, concentrate primarily on precise keyword pairing, which is ineffective in capturing document information. During the course of this article, a solution is based on two techniques: a fully unique Search Public Encryption (SPE) scheme that supports semantic multi-keyword searches over encrypted data, and a totally unique Search Public Encryption (SPE) scheme that supports semantic multi-keyword searches over encrypted data which is shallow neural network model called “word2vec”. The keywords conversion method, on the other hand, transforms keywords into a collection of vectors, for capturing semantic keywords from files.It then encrypts these transformed vectors and creates the target SPE scheme using an effective inner product encryption scheme. Furthermore,analysis, both theoretically and experimentally, is provided to check the scheme's performance and precision.Discoveries with data from real-life situations show that the system is capable of achieving a realistic performance in terms of time and space complication . For the first time in a general public key environment, a functional keywords search scheme has been developed over sensitive messages.

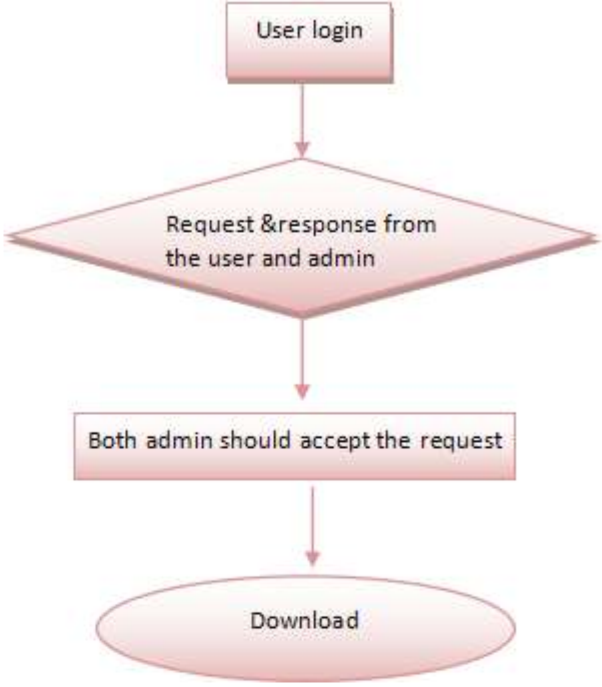
Run Xie,Chunxiang Xu, Fagen Li;[7] Due to the extreme increasing understanding of information protection, before being transmitted to the cloud, sensitive information is normally encrypted. The keyword-searchable public-key encryption search offers an effective method for retrieving encrypted data without the need for symmetric encryption's complicated key management. As a result, it's an essential strategy for encouraging safe and reliable cloud storage. Regrettably, there is only one cipher - text attempted to restore that is safe from within keyword guessing assaults (KGA). A structure to protect against insider attacks is described in this paper.. In addition, a delegated tester (dCRKS) is proposed for keyword quest for effective cipher - text recovery that is safe against.inside.keyword.guessing attacks (KGA). The scheme's safety evidence and performance.analysis prove that it is ideal for downloading data from a public cloud.

Yang Lu; Jiguo Li[8] ; Yichen Zhang, used the Searchable.encryption which is a modern cryptographer concept that allows a knowledge storage database to extract information cipher-texts without knowing what they're looking for or what the data cipher-texts are looking for. SCF-PEKS (Safe Channel Free PEKS) is a useful addition. PEKS stands for public key encryption with keyword search, and it eliminates the requirement that the search keyword be communicated to the info secret communication channels between the storage server and the client. However, the current SCF-PEKS architecture is vulnerable to the keyword guessing (KG) attack, which means that keyword searches are not private. As an improvement to the SCF-PEKS system, free public key encryption with privacy-preserving keyword search on the open channel (SCF-PEPCKS) framework is proposed in this paper. The system effectively addresses the SCF-PEKS framework's safety flaw and provides resistance to documented KG attacks. Without the use of random oracles, a concrete SCF-PEPCKS scheme. The security proofs show that it provides keyword cipher-text,both the malicious data management server and the malicious data storage server and, as a result, the external attacker are protected by trapdoor privacy. The comparisons, as well as the experimental findings,specify that the proposed SCF-PEPCKS system is both secure and feasible.

Takanori Saito, Toru Nakanishi;[9]To scan encrypted cloud storage for keywords, PEKS is a proposal for public-key encryption with keyword quest.. The PEKS is eventually Keyword Guessing Attack (KGA) vulnerability: Using the overall public key, everyone, even any keyword's cipher-text can be computed by the server..As a consequence, a server that is malicious will prepare potential keyword cipher-texts to verify if a trapdoor's keyword sent from the receiver is equal to the keywords of the cipher-texts that have been prepared. A fresh start form of PEKS, designated-recipients PEKS, is introduced in this paper, and it is secure against KGA. As a result, the malicious server is unable to launch KGA because no keyword can be encrypted. Also being created is a PEKS system with designated-senders and broadcast encryption.

3. ISSUES ADDRESSED

Challenges in the world of data storage are voluminous. Few such issues are the human errors, virus attacks, computer theft, disasters, hackers and insiders, etc.Here we address the vulnerability of the keyword search when kept common between a group of workers in spite of the file being encrypted. Once the permission is granted to too many workforce the data becomes vulnerable by default.Thus creating an hierarchy between the admin level helps the owner to safeguard the data. The implementation of Diffie-Hellman algorithm maintains the security of the key provider and prevents unwanted access.


User login
Request &response from the user and admin
Both admin should accept the request
Download

System Flow

4. PROPOSED SYSTEM

The system has used algorithms to ensure the low key workers should not know about their key provider and the owner who can only upload the file can overview the activities on the access of the files stored. The encryption process will provide the key to the user only after the identification is verified through levels by the Admins. The user can view and download the file but cannot upload or edit any content in them making the files non-editable and tight.The users once registered are stored in the data table and their actions are recorded for future purpose. This is common for both the owner and the user. The Diffie- Hellman algorithm is introduced, which ensures that the user doesn't know the key provider. Thus, ensuring the owner about the data security

5. MODULE DESCRIPTION

A. User Interface

This module is the front end of the system, which deals with the user registration and login activity. It is developed for security purposes. To enter the system the user must log into the page and their credentials are verified displaying a success message if they are claimed to be right. If the credentials are not verified, the window displays an invalid message. This activity prevents unauthorized users from accessing the data. The login window is created for the owner, user, admin-1 and admin-2. The verification process happens with the help of the stored data of the user. Thus this login process also helps the owner to monitor the user activity creating a hierarchy in the system,(fig-1) which manages to keep the owner informed about the data access. Thus, introducing the monitoring system is associated with the login. The module is designed with the help of javascript.

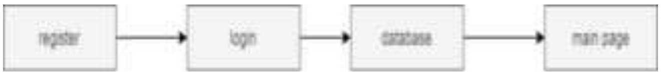


Fig. 1: User interface

B. File upload

Once the owner authorization is complete he is given the privilege of uploading the files to the cloud. This action can be performed only by the owner of the organization. The addition or removal action is specified to the authorized owners(fig-2). The files once uploaded are stored in the cloud and their details are recorded in the database for future reference and easy identification. This module is developed with the help of SQL.

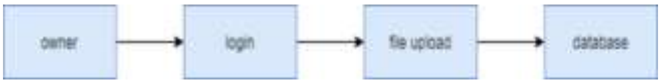


Fig. 2: File Upload

C. Encryption process

This module is a key element of the project that works at the back end of the system. Once the file is uploaded by the owner, it is usually encrypted before being uploaded. The encryption process takes place in this module. The encryption process is integrated by the Diffie-Hellman algorithm. Thus it ensures the key is circulated only between two people. It can also be called the end to end encrypted process(fig-3). Not even the monitoring head can view the key making it that private is the aim of the module.

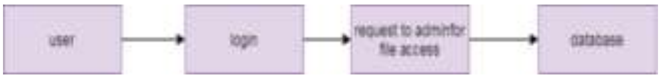


Fig. 3: Encryption Process

D. Request to admin

The access to view the uploaded files has to be provided by the admins. The user has to register themselves with their credentials which include their name, email id, phone number and their personalized password. Once the registration is complete their data is stored in the database which is cross verified at the time of login. The cross enquiry is done by the admin-1 with the username and password provided by the user. Furthermore the user login request is forwarded to the admin-2(fig-4).

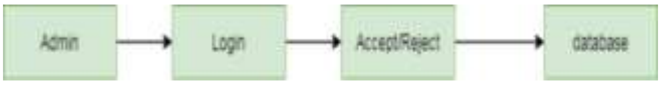


Fig. 4: Request to Admin

E. Response From Admin

Once the admin-1 forwards the user login request to admin-2, the job of admin-2 is to re-verify the user based on their advanced data such as their phone number or email id. Therefore the user will provide their email id or phone number to admin-2, who will evaluate it from the database concluding whether the user is authorized or not. If the user login is verified successfully the admin will provide them with the key to access the files. Else not the user login will display a failure message(fig-5).

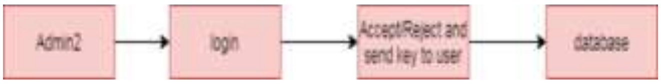


Fig. 5: Response From Admin

F. Download the files

Once the user is verified and is provided with the key he/she can download the file. The authorized user can only view and download the file but cannot edit or upload the file from their end which makes the system more secure(fig-6).

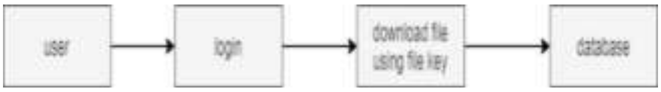


Fig. 6: Download the Files

4. ALGORITHM

Only if the public key's validity is guaranteed is a public key encryption scheme secure.A basic public key algorithm is Diffie-Hellman key exchange.

1.Using a discrete algorithm-based public key scheme, the procedure allows two users to create a secret key.

2.The protocol is only reliable if the two participants' identities can be verified.

There are two public options for this scheme:

● l q is a prime number.

● l A primitive root of q expressed as an integer.

(Note: The primordial P's source is one , and all images from 1 to P-1 are produced by the power-module P.).

3.Assume that users c and d want to swap keys.

User c chooses an Integer at random $X c lt q$ and calculates.

$Y c = X c mod q$

.4.User d selects a random integer $X d lt q$ and computes **$Y d = X d mod q$** independently.

5.Each side holds the X value private while making the Y have a public benefit, accessible to the other. User c calculates the key as follows:

$k = (Y_d)^{X_c} mod \ q$

User b computes the key as :

$k = (Y_c)^{X_d} mod \ q $

The calculations produce identical results :

$k = (Y_d)^{Xc} mod \ q -\gt \text{calculated by user a} \\ = (α^{Xd} mod \ q)^{Xc} mod \ q \\ = (α^{Xd})^{Xd} (mod \ q) -\gt \text{By rules of modular arithmetic} \\ = α^{Xd \ Xc} mod \ q \\ = (α^{Xc})^{Xd} mod \ q$

$k = (α^{Xc} mod \ q)^{Xd} mod \ q$

The proposed system develops a public key tree with the help of Hierarchical Public key encryption with keyword search providing a tree structure to the access of the data restricting few activities to the low-key users.

5. ADVANTAGES

The system provides security to the data by ensuring the key is not shared between the users.

The monitoring system provides the owner with the access activity of the users.

The methodologies predicted are safe and secure.

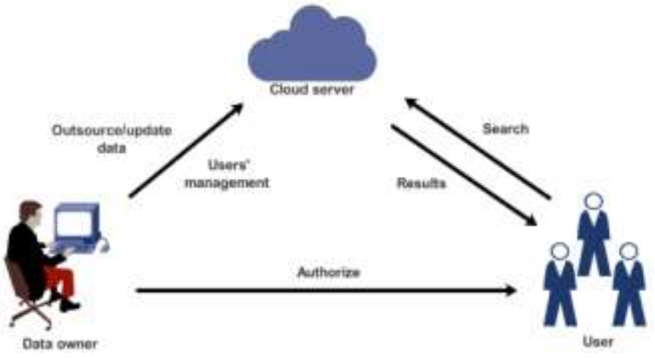


FIG-8- SYSTEM DESCRIPTION

6. RESULT AND CONCLUSION

The system proposed has addressed the issues of IKGA making the organisation threatless of data integrity. The algorithm integrated with the system ensures the key provider is unknown and secured. The file upload activity is restricted to the authorized owner making the user freezed under the section. The user can enter the page after a process of dual verification creating a hierarchical structure. Thus, preventing the unauthorised user from accessing the files. The owner can monitor the user activity making it more easy for the owner to identify the attacker. Experiments display that the scheme proposed is efficient enough to provide security to the data.

7. REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Eurocrypt, vol. 3027. Springer, 2004, pp. 506–522.

[3] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Transactions on computers, vol. 62, no. 11, pp. 2266–2277, 2013.

[4] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in Australasian Conference on Information Security and Privacy. Springer, 2015, pp. 59–76.

[5] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vol. 403, pp. 1–14, 2017.

[6] Yu Zhang ; Yifan Wang ; Yin Li Searchable Public Key Encryption Supporting Semantic Multi-Keywords Search. 2019

[7] Run Xie ; Chunxiang Xu ; Fagen Li ;Cipher text retrieval against insider attacks for cloud storage.2017

[8] Yang Lu ; Jiguo Li ; Yichen Zhang SCF-PEPCKS: Secure Channel Free Public Key Encryption With Privacy-Conserving Keyword Search. 2017

[9] Takanori Saito ; Toru Nakanishi Designated-Sender's Public-Key Searchable Encryption Secure against Keyword Guessing Attacks.2018

[10] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Information Sciences, vol. 238, pp. 221–241, 2013.