iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44367

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Secure Cloud Storage with a Traceable Authorization System Using KGC

Mrs. R Sivaranjani M.E[1], Mr. Arun Kumar L[2], Mr. Karankumar R[3], Mr. Meiyarasu S[4]
[1]*Assistant Professor, Department of Computer Science and Engineering, Tamilnadu College of Engineering, Coimbatore.*
[2, 3, 4]*Final Year, Department of Computer Science and Engineering, College of Engineering, Coimbatore.*

Abstract: ***Various types of encryption algorithms are used to protect information from unwanted exposure and to guarantee data confidentiality and secure storage. As a result, keyword-based searching has been introduced, in which the requested file is found following a search using the corresponding keyword. As a result, finding and revoking the malicious user who is abusing the secret key must be resolved as soon as possible. If a user tries to enter the erroneous key, the system considers him a bad user, and the user's privileges are promptly revoked. This project is primarily concerned with user authentication in order to strengthen the security system.***

Index Terms: ***Authorized search able encryption, traceability, verifiable outsourced decryption, key escrow free, multiple keywords subset search***

I. INTRODUCTION

Cloud computing [1], which provides convenient, on-demand services from a shared pool of configurable computing resources, has emerged as the most notable new computing paradigm. As a result, a rising number of businesses and people are opting to store their data on cloud servers. Despite the significant financial and technical benefits, very high security and privacy concerns [2],[3] have emerged as the most significant barrier to widespread adoption of data storage in public cloud infrastructure. Encryption is a key way for protecting data privacy when it is stored in a remote location [4]. However, due to the inability of cypher text to be read, how to properly execute keyword search for plaintext becomes problematic for encrypted data. Keyword search over encrypted data is possible with searchable encryption[5],[6].

Fine-grained search authorization is a desirable capability for data owners to share their private data with other authorized users in a file sharing system, such as a multi-owner multiuser scenario. However, the majority of existing systems [7],[8] demand that the user complete a huge number of difficult bi linear pairing operations. These overburdened computations place a significant demand on the user's terminal, which is particularly problematic for energy-constrained devices. The user can retrieve the message with ultra lightweight decryption [10], using the outsourced decryption method [9]. However, due to a malicious attack or system failure, the cloud server may deliver incorrect half-decrypted information. As a result, ensuring the validity of outsourced decryption in public key encryption with key management is critical.

The authorized entities may profit by illegally disclosing their private key to a third party. Assume a patient learns one day that a secret key pertaining to his electronic medical data is being auctioned on eBay. Such heinous behavior puts the patient's data privacy at risk. Even worse, if the insurance company or the patient's employer misuses confidential electronic health data containing critical health diseases, the patient's medical insurance or labour contracts will be terminated. The deliberate secret key leak age gravely jeopardizes authorized access control and data privacy protection.. As a result, identifying the malicious user, or even proving it in court, is critical. The secret key of a user is associated with a set of attributes rather than the individual's identity in an attribute-based access control system. It's difficult to track down the original key owner because the search and decryption authority can be shared by a group of users who share the same set of qualities . The importance of providing traceability to a fine-grained search authorization mechanism was overlooked in prior searchable encryption systems [7],[8].

More crucially, in the original PEKS method, the key generation centre (KGC) creates all of the system's secret keys, resulting in the key escrow dilemma. That is, the KGC has access to all of the users' secret keys and may thus search and decrypt all encrypted files without their knowledge, posing a serious threat to data security and privacy. In addition, when PEKS' traceability capability is implemented, the key escrow problem creates a new challenge. If a secret key is discovered to be for sale and the owner's identity (i.e., the traitor) is discovered, the traitor may claim that the secret key was leaked by KGC If the key escrow problem is not solved, there is no technological technique to determine who is the genuine traitor.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

II. RELATED WORK

A. Searchable Encryption

Encrypted data can be searched using keywords. Bon giorno et al proposed the concept of public key encryption with keyword search (PEKS), which is useful for preserving the privacy of data that is outsourced. Data owners in PEKS schemes [7], [8] keep their files on a remote, un trusted data server in encrypted form. The data users ask for a keyword trapdoor to search the encrypted files, and the data server performs the search. PEKS systems could be used to create searchable audit logs, as Waters et al. [5] shown. Later, Xu et al. presented a broad framework for combining PEKS and fuzzy keyword search that was not based on any concrete implementation. Tang suggested a bilinear pairing-based multiparty searchable encryption system. To combat off-line keyword guessing attacks, Chen et al. incorporated the idea of "dual-server" into PEKS in 2016. To provide time-controlled authority delegation, Yang et al. added a time-release and proxy re-encryption method to the PEKS scheme. Using order-preserving symmetric encryption, Wang et al. [1] suggested a ranked keyword search technique for searchable symmetric encryption. Cao et al. devised a novel approach for achieving ranked search for multiple keywords. Encryption that can be searched is also being investigated further

B. DES

DES is a block cipher that encrypts data in 64-bit blocks. The key is 56 bits long, however it was originally 64 bits long. The key length is reduced by the bit positions [8].. The first 64-bit plain text block is passed to the Initial Permutation (IP) function in the first stage. 2. The plain text is used for the initial permutation. 3. The first permutation yields two permuted block halves: Left Plain Text (LPT) and Right Plain Text (RPT) (RPT). 4. LPT and RPT now individually go through a 16-round encryption process, each with its own key.

Using Key Transformation, a separate 48-bit Sub-key is produced from the 56-bit key. c. The RPT is expanded from 32 bits to 48 bits using the Expansion Permutation. c. The 48-bit key is now XOR'd with the 48-bit RPT, and the result is sent on to the next step. d. The S-box substitution is used to generate 32-bits from 48-bits. e. P-Box Permutation is used to permute these 32 bits. f. P-output Box's is XOR'd with the LPT's 32-bit output. g. The RPT is the result of the XOR (32 bits), and the old RPT is the LPT. Swapping is the term for this procedure.

Input keys are required by the system (64 bits). This will be translated to a binary value, after which a 56-bit key will be generated. In a 56-bit block, 1 bit is placed in every even location and 0 in every odd place. 1) Split the result into two halves (each with 28 bits) (C0 and D0) 2) Perform a left shift on the previous findings to get C1 and D1. 3) Determine the value of K1 in the equation K1= C1 || D1. Concatenation is shown by the pipes (||). 4) Concatenate C1 and D1 to get a 56-bit block, which you can then use as an input for the next cycle to get C2 and D2, C3 and D3, and so on. 5) In the 56-bit block, each even bit is replaced with a 1 and each odd position with a 0 bit.

Because of the triple processing, this approach is three times as strong as DES, but it is also three times slower. The Triple-DES algorithm is more defined than the DES method due to key length and is utilized in many applications. TDES is depicted in Figure 2 as a block diagram. Triple-DES encrypts and decrypts three times using the DES algorithm. To accomplish the Triple-DES operation, the task employs three DES blocks..

C. Traitor Tracing

Chore et al. developed traitor tracing to assist content distributors in identifying pirates. There is no method to prevent a genuine user from giving (or selling) his decryption key to others in the digital convention distribution system. The traitor tracing feature aids the distributor in locating the misbehaving user via a "tracing" algorithm, allowing him to pursue legal action against the owner of the disclosed private key.

Later, a traitor tracing mechanism is added to broad-cast encryption, allowing a sender to generate cipher text that can only be decrypted by users in the selected receiver set. The broadcaster can identify the traitor thanks to the traceability feature, which also prohibits authorized users from releasing their keys. The strategy is to assign each user a unique set of keys that can be used as a "watermark" for tracing. For broadcast encryption, traceability is examined further. Over IDs, secret keys are not defined. Instead, they are linked to a collection of characteristics. The same set of qualities may be shared by many users. This makes expressive access control more convenient. Given a leaked secret key, however, determining the original key owner is impossible. It nearly guarantees that the malicious user who sells his private key will not be recognized. The CP-ABE traceability problem is investigated. It's difficult to implement in software while keeping both performance and security in mind.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

III. SYSTEM ARCHITECTURE

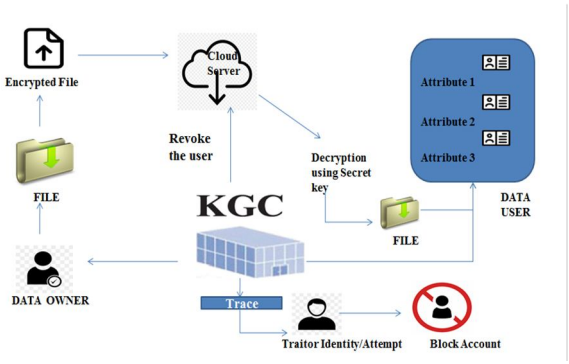


Fig.3.1.Architecture

IV. METHODOLOGIES

The user's secret key is encoded in each data collection. The data user can search an encrypted file saved in the cloud using the secret key. The keyword is then encrypted and sent to the trapdoor using the users' secret key. To achieve fine-grained access, the access policy is specified and incorporated into a cipher text during the encryption procedure. When a user's secret key is leaked for financial or other reasons, (KGC) uses an algorithm to track down the malicious user, after which it sends a revocation request to the cloud server to disable the user's search privileges. The decryption action is partially outsourced to a cloud server, and the data user can verify the correctness of the half-decrypted result. It increases efficiency and reduces the computational overhead of users' terminals significantly.

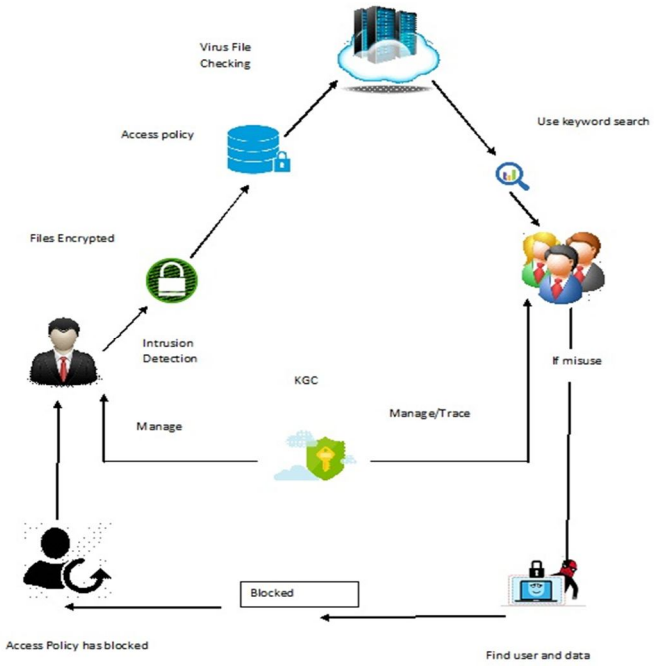


Fig.4.1.Working of Proposed System

If user1 has a file that is encrypted with the DES algorithm, the file will be encrypted with some access policy as a secret key, which will check the file for viruses. User2 need a file from user1 in order to make a request to their user1. The file will be generated after user1 accepts the request, and the Key Generation Centre will provide the secret key to user2 through mail. After that, user2 types the secret and keyword search that user1 has provided. Only a keyword match will allow you to download the file before the modification date expires; otherwise, the query will be refused, and the file will be decrypted as plain text. The user2 will be identified as a malicious individual, and if they try to access the bogus websites several times, they will be marked as such. When he tries to click any link, the menu appears to be briefly blocked..

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

V. MODULE DESCRIPTION

There are various types of modules, that are

1) Data Owner
2) Cloud User
3) File Searching
4) Cloud Server
5) Key Generation Centre (KGC).
6) Traitor Tracing
7) Intrusion Detection And Prevention

A. Data Owner

The files are stored on a cloud storage service by the data owner. The data owner takes the keyword set from the file and encrypts it into a secure index before outsourcing the data. The document is also cipher text encrypted. To provide fine-grained access control, the access policy is specified and incorporated into the cipher text during the encryption process as shown in the flowchart in fig 5.1.1 and the screenshot in fig 5.1.2.

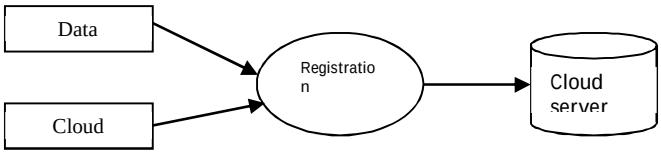


Fig.5.1.1.Flowchart for Data Owner

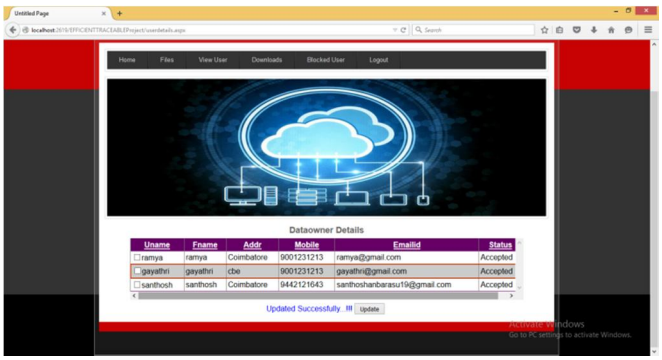


Fig.5.1.1.Screenshot for Data Owner

B. Cloud User

Each data user has a collection of attributes that describe his traits. The attribute set is stored in the secret key of the user. This module assists the user in searching the file using keywords and receiving an accurate result list based on the user's query as shown in the flowchart in fig 5.2.1 and the screenshot in fig 5.2.2.

.

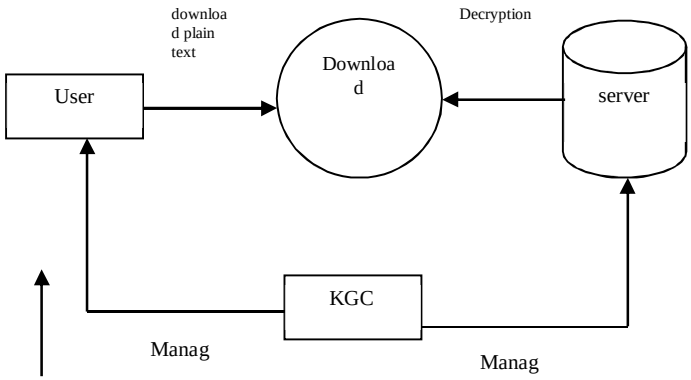


Fig.5.2.1.Flowchart for Cloud User

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Fig.5.2.2.Screenshot for Cloud User

C. File Searching

The data user can search the encrypted files saved in the cloud using the secret key, in which case he selects a keyword set to search. The user's private key is then used to encrypt the keyword into a trapdoor. The cloud server responds to the user's search query and identifies the matching files if the user's attribute set matches the access policy established in the encrypted files. The search query will be refused if this is not the case. The user then uses a decryption technique to recover the plaintext after receiving the match files as shown in the fig 5.3

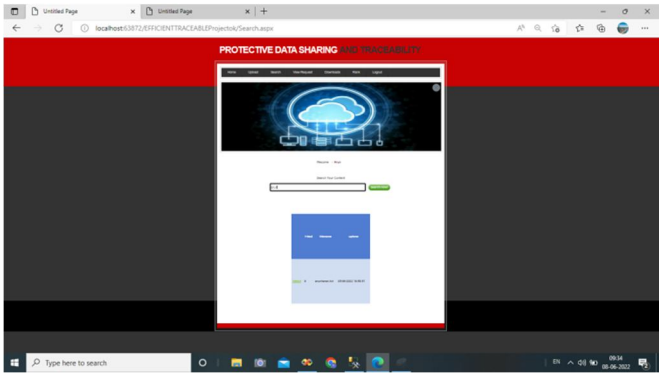


Fig.5.3.Screenshot for File Searching

D. Cloud Server

The cloud server has a lot of storage space and has a lot of computational capacity, so it can give on-demand support to the system. The data owner's encrypted files are stored on the cloud server, which also responds to the data user's search query as shown in the flowchart in fig 5.4.1 and the screenshot in fig 5.4.2.

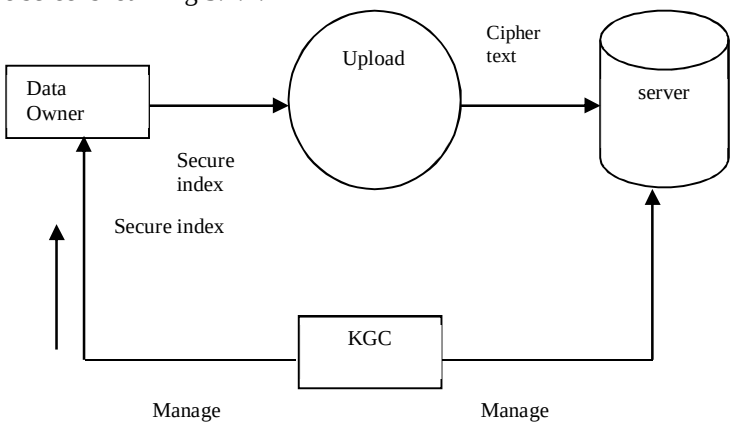


Fig.5.4.1.Flowchart for Cloud Server.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

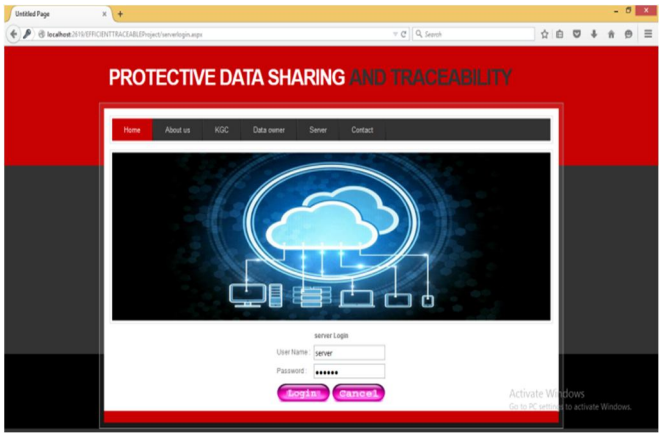


Fig.5.4.2.Screenshot for Cloud Server.

E. Key Generation Center (KGC)

KGC is in charge of generating the system's public parameter as well as the users' public/secret key pairs. KGC has access to all of the users' secret keys. As a result, all secret keys are escrowed to KGC, and the data user's secret key is known to both KGC and the user, a process known as "key escrow" as shown in the screenshot in fig 5.5

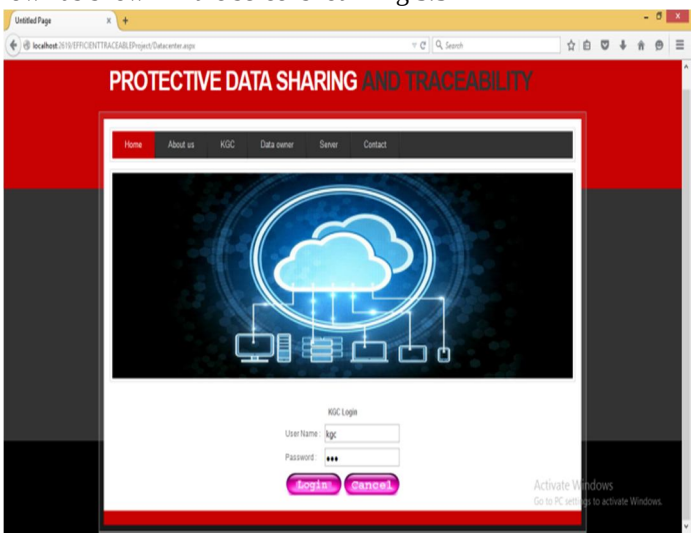


Fig.5.5.Screenshot for KGC Login

F. Traitor Tracing

KGC uses the tracing algorithm to discover the malicious user when the user's private key is released for profit or other reasons. KGC sends a user revocation request to the cloud server after locating the traitor to revoke the user's search privileges. The broadcaster can identify the traitor thanks to the traceability feature, which also prohibits authorised users from releasing their keys as shown in the flowchart in fig 5.6.1 and the flow diagram in fig 5.6.2.

.

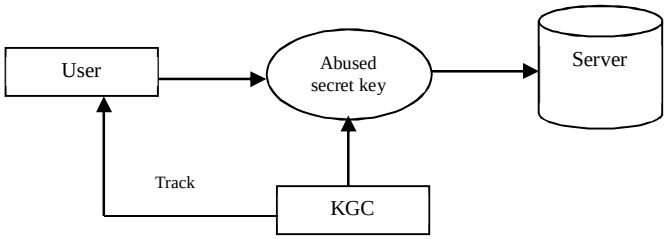


Fig.5.6.1.Flowchart for Traitor Tracing

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

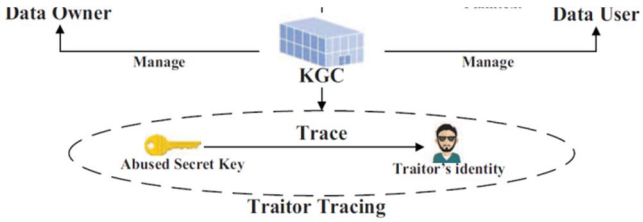


Fig.5.6.2.Flow Diagram for Traitor Tracing

G. Intrusion Detection and Prevention

The goal is to detect intrusions and attacks. Identity management is used to guarantee that only the appropriate level of access is allowed to the appropriate person. The cloud management team, data centre, and data owner are all notified via the intrusion detection area. Its security also gathers information about intrusions by activating alarms. The threats posed by incursions are numerous and varied. The rejection and warning e-mails will be written specifically for the data owner to receive. The process begins with a possible intrusion event (for example, unlawful access to data), which prompts the client process in this paradigm to compose an email/message to the cloud data administrator.

VI. CONCLUSION

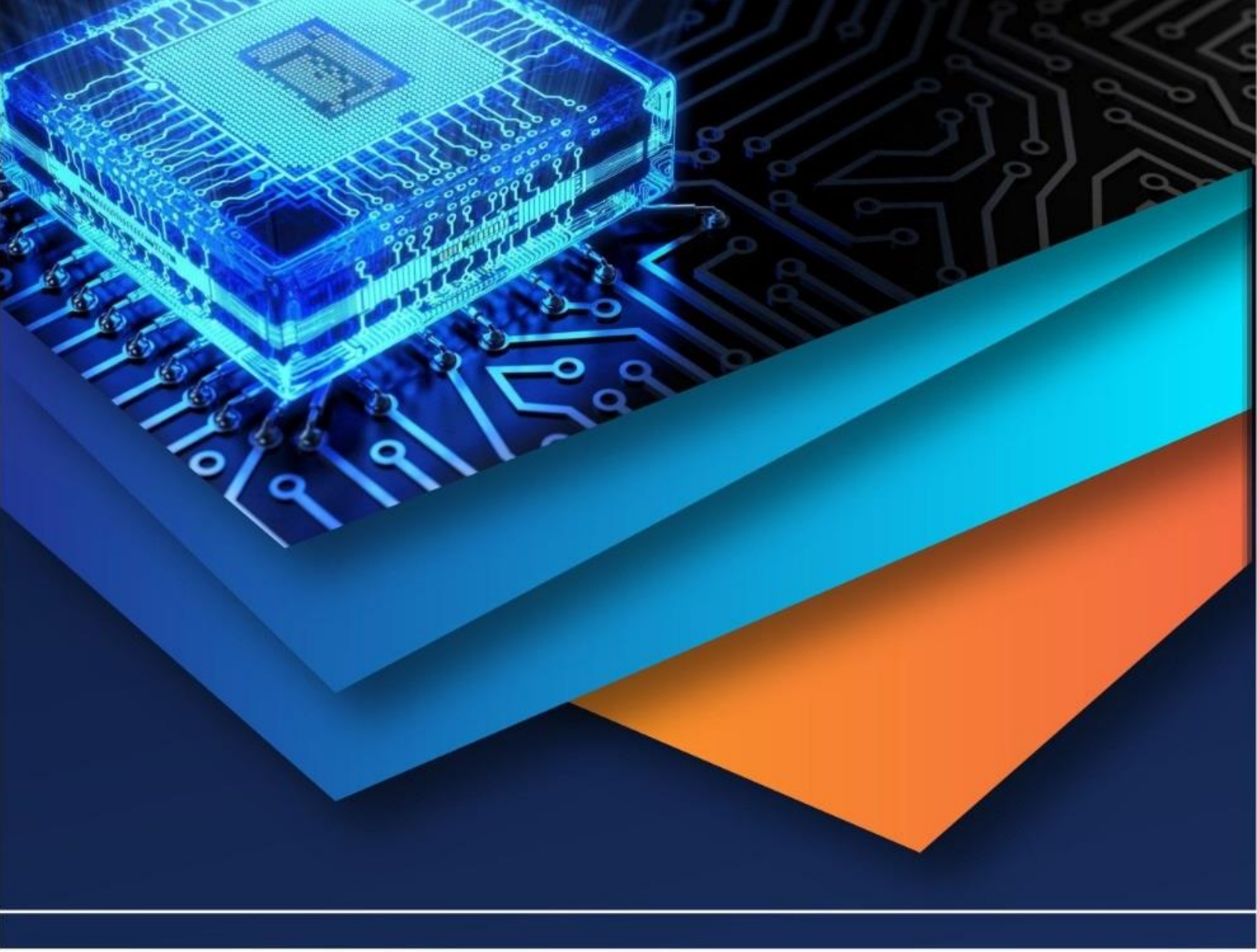
In a secure cloud storage system, access control is enforced and key-word search is supported. In this paper, we present a concrete construction for a new paradigm of searchable encryption system. It allows for customizable subset searches of numerous key phrases and overcomes the key escrow problem during the key generation process. A nefarious user whose private key may be traced for monetary gain. The decryption operation is outsourced in part to a cloud server, and the data user can check the accuracy of the half-decrypted output. Its efficiency in processing and storage overhead is demonstrated by performance study and simulation. The computational overhead of data user terminals was dramatically decreased in the experiments, saving a significant amount of energy for resource-constrained devices.

VII. FUTURE SCOPE

When a user accesses a secured document with another device, an alert is sent to the user's preferred phone number or email address. If two people logged in using the same credentials, the first one was logged out. If a user hasn't interacted with the website for a certain period of time, they will be automatically logged out. Given the file's accessibility, which allows the owner to control who can view the file while uploading it**.**

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ran, W. Lou. “Secure ranked keyword search over encrypted cloud data”[C]//IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2010:253-262.
[2] Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Dean. “Privacy-preserving Double-Projection Deep Computation Model with Crowd sourcing on Cloud for Big Data Feature Learning,” IEEE Internet of ThingsJournal,2017,DOI:10.1109/JIOT.2017.2732735.
[3] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, “Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2016, vol.11, no.4, 789-798.
[4] X. Liu, R. H. Deng, K. K. R. Chou, J. Wang. ”An efficient privacy preserving out sourced calculation toolkit with multiple keys.” IEEE Transactions on Information Forensics and Security 11.11 (2016):2401-2414.
[5] B. R. Waters, D. Bal fan z, G. Durfee, and D. K. Smatters, “Building an encrypted and searchable audit log,” in NDSS, 2004.
[6] Y. Yang, X. Liu, R. H. Deng, “Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language”. IEEE Transactions on Dependable and Secure Computing, 2018, publish online,DOI:10.1109/TDSC.2017.2787588.
[7] W. Sun, S. Yu, W. Lou, Y. Hoe and H. Li, “Protecting Your Right: Verifiable Attribute based Keyword Search with Fine IEEE Transactions on Parallel and Distributed Systems, 2016,vol.27, o.4, pp.1187-1198.
[8] Grained Owner-enforced Search Authorization in the Cloud,” K. Liang, W. Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981-1992.
[9] M. Green, S. Rosenberger, and B. Waters, “Outsourcing the decryption of ABE cipher texts,” in USENIX Security Symposium, ACM, 2011, pp.34-34.
[10] J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343-1354



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY