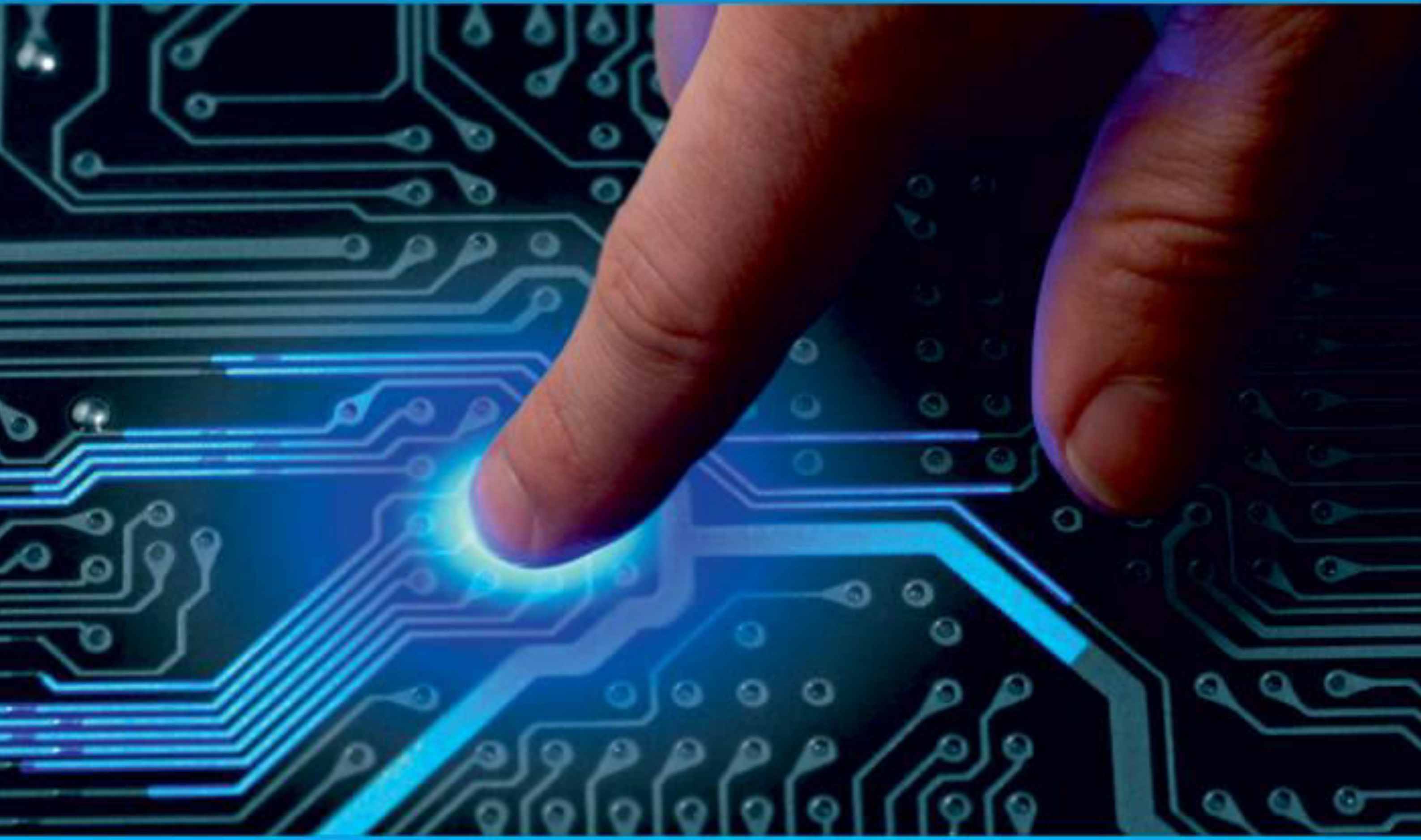
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105191 |

The Efficient Authorization Search System for Secure Cloud Storage

Dr.Bhuvaneshwari K V[1], Premraj S Ksheerasagar [2], Nisha D Mahendrakar[3], M Vidya Sagar[4] , Ruqsar Fatima[5]

Associate Professor, Department of Information Science and Engineering, BIET, Davanagere, Karnataka, India [1]

U.G. Students, Department of Information Science and Engineering, BIET, Davanagere, Karnataka, India [2,3,4,5]

ABSTRACT:Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (EF-TAMKS-VOD). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded. Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that EF-TAMKS-VOD is provably secure. Efficiency analysis and experimental results show that EF-TAMKS-VOD improves the efficiency and greatly reduces the computation overhead of users' terminals.

KEYWORDS:Cryptography, encryption, decryption, key generation centre (KGC), public key encryption,attribute-basedencryption.

I. INTRODUCTION

With the development of new computing paradigm, cloud computing becomes the most notable one, which provides convenient, on-demand services from a shared pool of configurable computing resources. Therefore, an increasing number of companies and individuals prefer to outsource their data storage to cloud server. Despite the tremendous economic and technical advantages, unpredictable security and privacy concerns become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure.

Encryption is a fundamental method to protect data privacy in remote storage. However, how to effectively execute keyword search for plaintext becomes difficult for encrypted data due to the unreadability of ciphertext. Searchable encryption provides mechanism to enable keyword search over encrypted data for the file sharing system, such as multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with another authorized user. The outsourced decryption method allows user to recover the message with ultra-lightweight decryption.

However, the cloud server might return wrong half-decrypted information as a result of malicious attack or system malfunction. Thus, it is an important issue to guarantee the correctness of outsourced decryption in public key encryption with keyword search (PEKS) system.

The authorized entities may illegally leak their secret key to a third party for profits. Suppose that a patient someday suddenly finds out that a secret key corresponding his electronic medical data is sold on e-Bay. Such despicable behaviour seriously threatens the patient's data privacy. Even worse, if the private electronic health data that contain serious health disease is abused by the insurance company or the patient's employment corporation, the patient would be declined to renew the medical insurance or labour contracts.

The intentional secret key leakage seriously undermines the foundation of authorized access control and data privacy protection. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice. In attribute-based access control system, the secret key of user is associated with a set of attributes rather than individual's identity. As the search and decryption authority can be shared by a set of users who own the same set of attributes, it is hard to trace the original key owner. Providing traceability to a fine-grained search authorization system is critical and not considered in previous searchable encryption systems.

More importantly, in the original definition of PEKS scheme, key generation centre (KGC) generates all the secret keys in the system, which inevitably leads to the key escrow problem. That is, the KGC knows all the secret keys of the users and thus can unscrupulously search and decrypt on all encrypted files, which is a significant threat to data security and privacy. Besides, the key escrow problem brings another problem when traceability ability is realized in PEKS.

If a secret key is found to be sold and the identity of secret key's owner (i.e., the traitor) is identified, the traitor may claim that the secret key is leaked by KGC. There is no technical method to distinguish who is the true traitor if the key escrow problem is not solved.

II. RELATED WORK

[1] Searchable Encryption-Searchable encryption enables keyword search over encrypted data. The concept of public key encryption with keyword search (PEKS) was proposed by Boneh et al, which is important in protecting the privacy of outsourced data. Data owners in PEKS schemes store their files in encrypted form in the remote untrusted data server. The data users query to search on the encrypted files by generating a keyword trapdoor, and the data server executes the search operation. Waters et al. showed that PEKS schemes could be utilized to construct searchable audit logs. Later, Xu et al. presented a general framework to combine PEKS and fuzzy keyword search without concrete construction. Tang proposed a multiparty searchable encryption scheme together with a bilinear pairing-based scheme. In 2016, Chen et al. introduced the concept "dual server" into PEKS to resist off-line keyword guessing attack. Yang et al. introduced time-release and proxy re-encryption method to PEKS scheme in order to realize time-controlled authority delegation. Wang et al. proposed a ranked keyword search scheme for searchable symmetric encryption, in which the order-preserving symmetric encryption is utilized. Cao et al. designed a novel system to realize multiple keywords ranked search. Searchable encryption is also further studied.

[2] ABE (Attribute Based Encryption)- ABE is an important method to realize fine-grained data sharing. In ABE schemes, descriptive attributes and access policies are associated with attribute secret keys and ciphertexts. A certain secret key can decrypt a cipher text if and only if the associated attributes and the access policy match each other. The notion of ABE was proposed by Sahai et al. in 2005. According to whether the access control policy associates with the ciphertext or the secret key, ABE schemes can be classified into ciphertext-policy ABE (CPABE) and key-policy ABE (KP-ABE). Since the Sahai's seminal work, ABE based access control becomes a research focus. Considering the challenges in expressing access control policy, ABE scheme with non-monotonic access structure is proposed. ABE systems with constant size cipher text are constructed to reduce the storage overhead. In order to accelerate the decryption, researchers make effort to speed up the decryption algorithm. Decentralized ABE is investigated in which multiple authorities work independently without collaboration.

[3] Traitor Tracing- Traitor tracing was introduced by Choretal. to help content distributors identifying pirates. In the digital content distribution system, there is no way to prevent a legitimate user to give (or sell) his decryption key to the others. Traitor tracing mechanism helps the distributor to find out the misbehaved user by running "tracing" algorithm so that he could take legal action against the owner of the leaked secret key. Later, traitor tracing mechanism is introduced to broadcast encryption, where a sender is able to generate ciphertext and only the users in the designated receiver set can decrypt. The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys.

The approach is to give each user a distinct set of keys, which is deemed as "watermark" for tracing. Traceability is further investigated for broadcast encryption in. In CP-ABE scheme, secret keys are not defined over identities. Instead, they are associated with a set of attributes. Multiple users may share the same set of attributes. This brings convenience to expressive access control. However, given a leaked secret key, it is impossible to figure out the original key owner in traditional ABE system. It means that the malicious user, who sells his secret key, almost has little risk of being identified. The traceability problem in CP-ABE is studied.

III. PROPOSED SYSTEM

EF-TAMKSVOD achieves fine-grained data access authorization and supports multiple keyword subset search. In the encryption phase, a keyword set KW is extracted from the file, and both of KW and the file are encrypted. An access policy is also enforced to define the authorized types of users. In the search phase, the data user specifies a keyword set KW0 and generates a trapdoor TKW0 using his secret key. In the test phase, if the attributes linked with user's secret key satisfy the file's access policy and KW0 (embedded in the trapdoor) is a subset of KW (embedded in the ciphertext), the corresponding file is deemed as a match file and returned to the data user. The order of keywords in KW0 can be arbitrarily changed, which does not affect the search result. EF-TAMKS-VOD supports flexible system extension, which accommodates flexible number of attributes. The attributes are not fixed in the system initialization phase and the size of attribute set is not restricted to polynomial bound, so that new attribute can be added to the system at any time. Moreover, the size of public parameter does not grow with the number of attributes. No matter how many attributes are supported in the system, no additional communication nor storage costs is brought to EF-TAMKS-VOD. This feature is desirable for the cloud system for its ever-increasing user volume.

IV. METHODOLOGY

Data owner

Data owner utilizes the cloud storage service to store the files. Before the data outsourcing, the data owner extracts keyword set from the file and encrypts it into secure index. The document is also encrypted to ciphertext. During the encryption process, the access policy is specified and embedded into the ciphertext to realize fine-grained access control.

Data user

Each data user has attribute set to describe his characteristics, such as professor, computer science college, dean, etc. The attribute set is embedded into user's secret key. Using the secret key, data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search. Then, the keyword is encrypted to a trapdoor using user's secret key. If the user's attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on user's search query and finds the match files. Otherwise, the search query is rejected. After the match files are returned, the user runs decryption algorithm to recover the plaintext.

Key generation centre

KGC is responsible to generate the public parameter for the system and the public/secret key pairs for the users. Once the user's secret key is leaked for profits or other purposes, KGC runs trace algorithm to find the malicious user. After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user's search privilege.

Cloud server

Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system. Cloud server is responsible to store the data owner's encrypted files and respond on data user's search query.

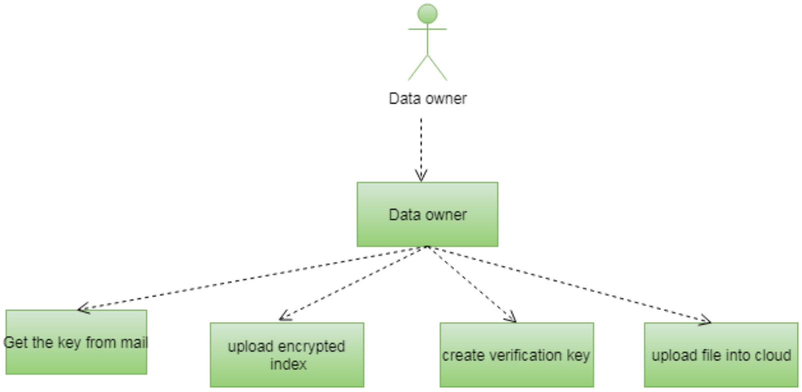


Fig 1.1Data owner

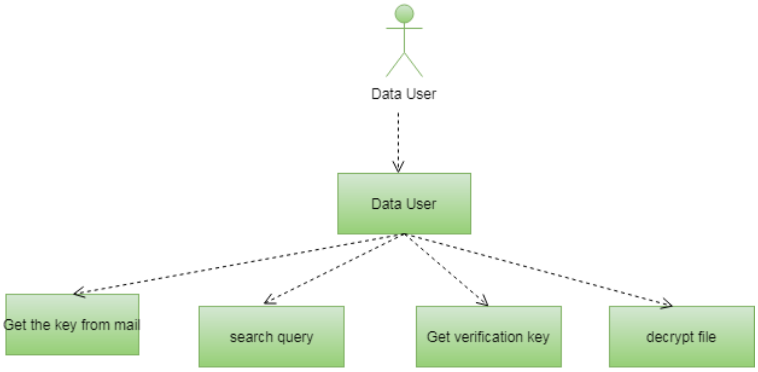


Fig 1.2 Data user

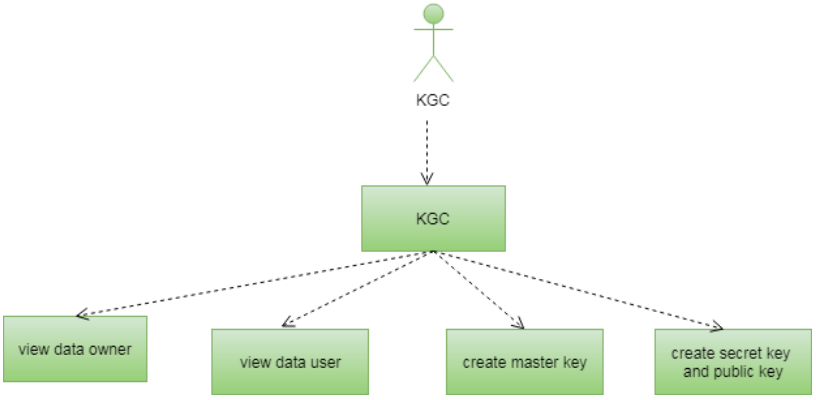


Fig 1.3KGC (Key Generation Centre)

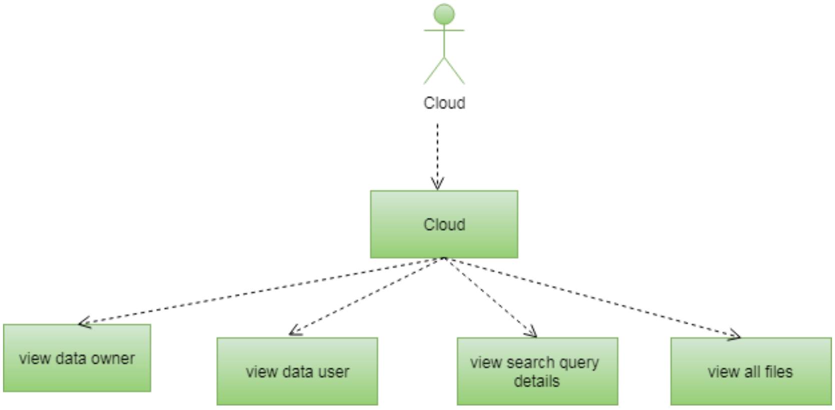
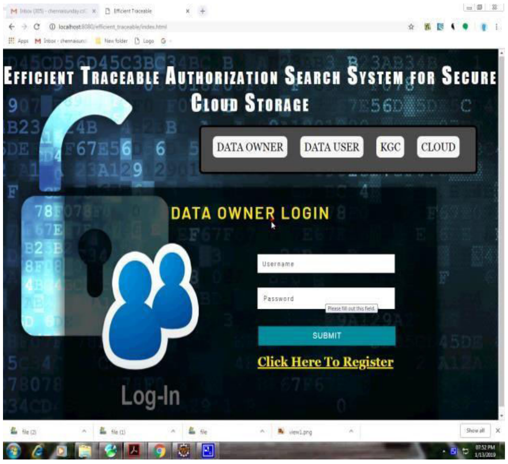


Fig 1.4 Cloud

V. EXPERIMENTAL RESULTS

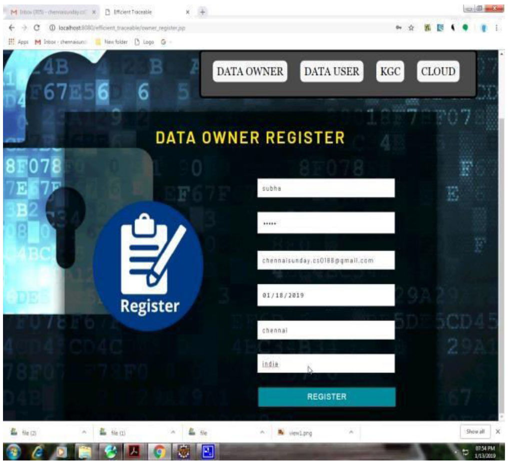
There is a login page that allows the data owner, data user, KGC, and cloud admin to log in as shown in fig 2. If the data owner is new to the system, they must register before gaining access to the login functionality as shown in fig 3. Once successfully logged in, the data owner's approval by the KGC admin is confirmed, and the master key is sent to the data owner's registered Gmail account. This master key enables the data owner to upload files securely as shown in fig 4 and fig 5. After successfully uploading a file and specifying the keyword index, the uploaded file is encrypted for enhanced security as shown in fig 6. When the data user logs in, they can request the key to access the data owner's file. The KGC admin then sends the public key and attribute key to the user's registered Gmail account as shown in fig 7. Upon receiving the public key and attribute key, the data user can access the file. To download the file in a decrypted form, the KGC will send the decryption key as shown in fig 8. Any attempt by an unauthorized user to access the file will be identified as an act of betrayal, and the admin can block that user fig 9. Additionally, the KGC admin has the ability to view the number of users who have accessed the file, presented in a bar graph format as shown in fig 10.

Results of the efficient authorization search system for secure cloud storage.


Efficient Traceable Authorization Search System for Secure Cloud Storage

DATA OWNER LOGIN

Fig 2Data owner login


DATA OWNER REGISTER

subha

•••••

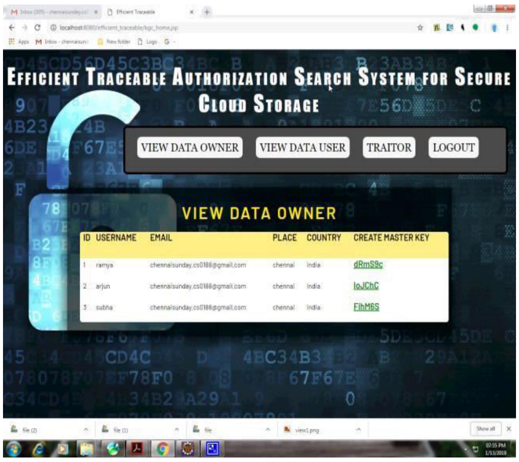
chennaisunday.cs0188@gmail.com

01/18/2019

chennai

india

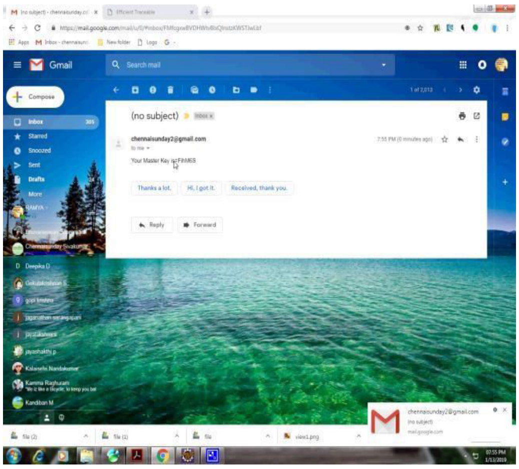
Fig 3 Data owner registration


EFFICIENT TRACEABLE AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE
VIEW DATA OWNER
VIEW DATA USER
TRAITOR
LOGOUT

VIEW DATA OWNER

ID	USERNAME	EMAIL	PLACE	COUNTRY	CREATE MASTER KEY
1	ramya	chennaisunday.cs0188@gmail.com	chennai	india	dRmS9c
2	arjun	chennaisunday.cs0188@gmail.com	chennai	india	loJChC
3	subha	chennaisunday.cs0188@gmail.com	chennai	india	FIhM6S

Fig 4 View Data owner

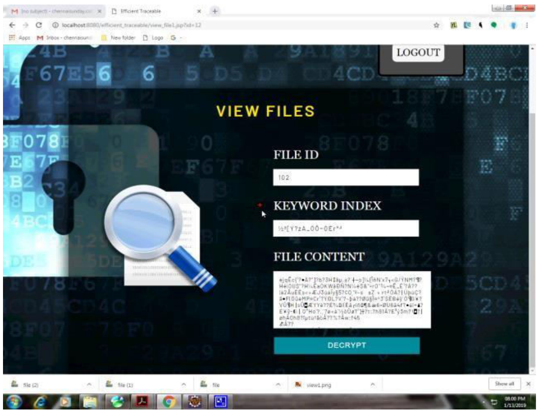


(no subject) Inbox

chennaisunday2@gmail.com
to me
7:55 PM (0 minutes ago)

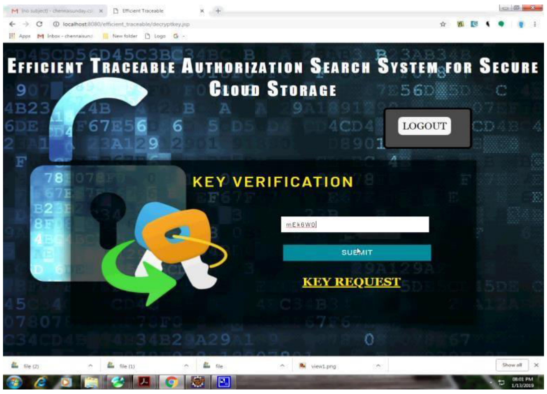
Your Master Key is=FIhM6S

Fig 5 Generated master key is sent to owner



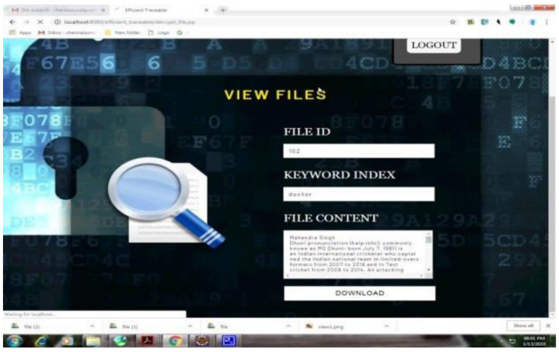
FILE ID: 102

Fig 6Encrypteddata is uploaded


EFFICIENT TRACEABLE AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE
LOGOUT
KEY VERIFICATION
SUBMIT
KEY REQUEST

mEk6W0

Fig 7 User requesting key to access upload data by owner.

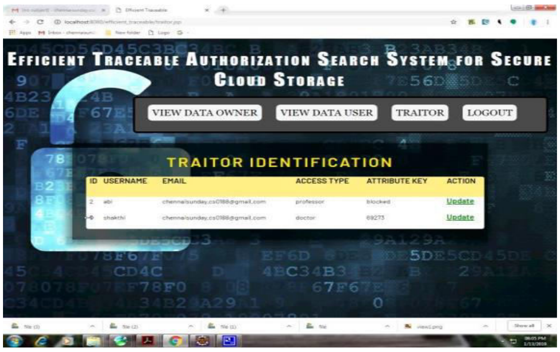


FILE ID: 102

KEYWORD INDEX: doctor

FILE CONTENT: Mahendra Singh Dhoni pronunciation (help·info); commonly known as MS Dhoni; born July 7, 1981) is an Indian international cricketer who captained the Indian national team in limited-overs formats from 2007 to 2016 and in Test cricket from 2008 to 2014. An attacking

Fig 8Decryption of the data


EFFICIENT TRACEABLE AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE
VIEW DATA OWNER
VIEW DATA USER
TRAITOR
LOGOUT

TRAITOR IDENTIFICATION

ID	USERNAME	EMAIL	ACCESS TYPE	ATTRIBUTE KEY	ACTION
2	abi	chennaisunday.cs0188@gmail.com	professor	blocked	Update
6	shakthi	chennaisunday.cs0188@gmail.com	doctor	69273	Update

Fig 9 Traitor identification

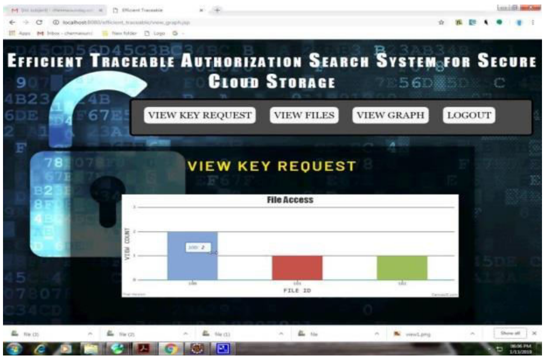


Fig 10 View key request

VI. CONCLUSION

The enforcement of access control and the support of keyword search are important issues in secure cloud storage system. In this work, it defines a new paradigm of searchable encryption system, and proposed a concrete construction. It supports flexible multiple keywords subset search, and solves the key escrow problem during the key generation procedure. Malicious user who sells secret key for benefit can be traced. The decryption operation is partly outsourced to cloud server and the correctness of half-decrypted result can be verified by data user. The performance analysis and simulation show its efficiency in computation and storage overhead. Experimental results indicate that the computation overhead at user's terminal is significantly reduced, which greatly saves the energy for resource-constrained devices.

REFERENCES

[1]. Q. Chai and G. Gong, "Verifiable symmetric searchable encryptionforsemihonest- but-curious cloud servers," in Communications (ICC), 2012 IEEE International Conference on.IEEE, 2012, pp. 917– 922.
[2]. S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keywordsearch for confidential investigation of remote forensics," in Multimedia InformationNetworking and Security (MINES), 2011 ThirdInternational Conference on. IEEE, 2011, pp.595–599.
[3]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikey word rankedsearch over encryptedcloud data," Parallel and Distributed Systems, IEEE Transactions on,vol. 25, no. 1, pp. 222–233, 2014.
[4]. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy searchover encrypted data inthe cloud," in INFOCOM, 2014 Proceedings IEEE.
[5]. L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds:towards a cloud definition,ACM SIGCOMM Computer Communication Review, vol. 39, no.1, pp. 50–55,2008.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com