AN AUTHENTICATED AND SECURED SEARCHING SYSTEM FOR CLOUD STORAGE ENVIRONMENT

Ms. Chandrika Gopisetty[1], Mr. Katti Jaya Krishna[2*]

1 Final Year MCA Student, QIS College of Engineering and Technology, Ongole

2 Assistant Professor, MCA Dept., QIS College of Engineering and Technology, Ongole*

Abstract: Secure inquiry over encoded remote information is urgent in distributed computing to ensure the information protection and ease of use. To anticipate unapproved information utilization, fine-grained get to control is essential in multi-client framework. Notwithstanding, approved client may purposefully release the security key for money related advantage. In this manner, following and denying the vindictive client who manhandles mystery key should be tackled unavoidably. 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 system could successfully keep the key generation center (KGC) from deceitfully seeking and unscrambling all scrambled records of clients. Likewise, the decoding procedure just requires ultra lightweight calculation, which is an alluring element for vitality constrained gadgets. What's more, effective client renouncement is empowered after the pernicious client is made sense of. Additionally, the proposed framework can bolster adaptable number of qualities instead of polynomial limited. Adaptable numerous catchphrase subset seek design is acknowledged, and the difference in the inquiry watchwords request does not influence the query item. Security investigation shows that EF-TAMKS-VOD is provably secure. Effectiveness examination and trial results demonstrate that EF-TAMKS-VOD improves the proficiency and enormously lessens the calculation overhead of clients' terminals.

Keywords: *Key Generation Center, Cloud Computing, Security.*

I. INTRODUCTION

WITH the improvement of new processing worldview, distributed computing [1] turns into the most eminent one, which gives advantageous, on-request benefits from a shared pool of configurable computing resources. Therefore, an expanding number of organizations and people like to redistribute their information stockpiling to cloud server. Regardless of the colossal monetary and specialized preferences, capricious security and protection concerns [2], [3] become the most conspicuous issue that blocks the far reaching reception of information stockpiling in open cloud framework. Encryption is a key strategy to ensure information protection in remote stockpiling [4]. Be that as it may, how to successfully execute keyword search for plaintext becomes difficult for encrypted information because of the ambiguity of ciphertext. Accessible encryption gives component to empower catchphrase look over encoded information [5], [6]. For the file sharing framework, for example, multi-proprietor multiuser situation, fine-grained look approval is an attractive capacity for the information proprietors to impart their private information to other approved client. In any case, a large portion of the accessible frameworks [7], [8] require the client to play out a lot of complex bilinear matching tasks. These overpowered calculations become a substantial weight for client's terminal, which is particularly genuine for vitality compelled gadgets. The re-appropriated decoding technique [9] enables client to recuperate the message with ultra lightweight unscrambling [10], [11]. Notwithstanding, the cloud server may return wrong half-unscrambled data because of noxious assault or systemmalfunction.Thus,itisanimportantissuetoguaranteethecorrectnessofoutsourceddecryptioninpublickeyencryption with catchphrase look (PEKS) framework [12]. The approved substances may unlawfully release their mystery key to an outsider forprofits[13].Supposethatapatientsomeday suddenlyfindsoutthatasecretkeycorrespondinghiselectronicmedicaldataissoldoneBay.Suchdespicablebehaviorseriouslythreatensthepatient'sdataprivacy.Even more awful, if the private electronic wellbeing information that contain genuine wellbeing ailment is manhandled by the insurance agency or the patient's business company, the patient would be declined to restore the therapeutic protection or work contracts. The purposeful mystery key spillage genuinely undermines the establishment of approved access control and information security assurance. Consequently, it is incredibly critical to

distinguish the vindictive client or even demonstrate it in a court of equity. In characteristic based access control framework, the mystery key of client is related with a lot of traits as opposed to person's personality. As the hunt and decoding specialist can beIEEE Transactions on Cloud Computing, Issue Date: 29.March.2018 shared by a lot of clients who possess a similar arrangement of characteristics, it is difficult to follow the first key proprietor [14], [15]. Giving recognizability [37] to a fine-grained seek approval framework is basic and not considered in past accessible encryption frameworks [7], [8], [12]. All the more essentially, in the first definition of PEKS conspire [12], key age focus (KGC) produces all the mystery enters in the framework, which definitely prompts the key escrow issue. That is, the KGC realizes all the mystery keys of the clients and hence can deceitfully look and decrypt on all encrypted files, which is a significant threat to information security and protection. Close to, the key escrow issue brings another issue when recognizability capacity is acknowledged in PEKS. On the off chance that a mystery key is observed to be sold and the character of secret key's owner (i.e., thetraitor) is identified, the traitor may guarantee that the mystery key is spilled by KGC. There is no specialized technique to recognize who is the genuine swindler if the key escrow issue isn't solved.1.1 Related Work 1.1.1 Searchable Encryption Searchable encryption empowers watchword look over scrambled information. The idea of open key encryption with catchphrase seek (PEKS) was proposed by Boneh et al [12], which is critical in securing the protection of redistributed information. Information proprietors in PEKS plans [7], [8], [16] store their files in encoded structure in the remote untrusted information server. The information clients inquiry to seek on the scrambled files by generating a keyword trapdoor, and the data server executes. Schemes could beutilized to construct search able auditlogs. Afterward, Xu et al. [17] introduced a general structure to join PEKS and fluffy catchphrase seeks without solid development. Tang [18] proposed a multiparty accessible encryption conspire together with a bilinear matching based plan. In 2016, Chen et al. [3] presented the idea "double server" into PEKS to oppose disconnected catchphrase speculating assault. Yanget al.[19] acquainted time-releaseand proxyreencryption technique with PEKS plot so as to acknowledge timecontrolled expert designation. Wang et al. [1] proposed a positioned catchphrase scan conspire for accessible symmetric encryption, in which the request saving symmetric encryption is used [35]. Cao et al. [36] planned a novel framework to understand different watchword positioned seek. Accessible encryption is likewise additionally contemplated in [20], [21], [22].1.1.2 ABE is a vital technique to acknowledge fine-grained information sharing. In ABE plans, elucidating traits and access approaches are related with quality mystery keys and ciphertexts. A specific mystery key can unscramble a ciphertext if and just if the related traits and the entrance strategy coordinate one another. The idea of ABE was proposed by Sahaietal. [23in2005. 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 [24 and key policy ABE (KPABE [25]. Since the Sahai'sseminal work, ABE based access control turns into an examination center [9], [10], [11], [26]. Considering the difficulties in communicating access control strategy, ABEscheme with non-monotonic access structure is proposed [27]. ABE frameworks with steady size ciphertext [28], [29] are built to decrease the capacity overhead. So as to quicken the decoding, analysts try to accelerate the unscrambling calculation [30], [31]. Decentralized ABE is researched in [32], in which various specialists work autonomously without collaboration.1.1.3 Traitor Tracing Traitor following was presented by Chor et al. [37] to help content wholesalers distinguishing privateers. In the advanced substance conveyance framework, there is no real way to keep a genuine client to give (or sell) his unscrambling key to the others. Double crosser following instrument encourages the merchant to find out the got into mischief client by running "following" calculation so he could make lawful move against the proprietor of the released mystery key. Later, traitortracing mechanism is introduced to broadcast encryption, where as end erisable to generate ciphertext and only the user sinthedesign ated receiversetc and ecrypt [38], [39]. The discernibility work empowers the supporter to recognize the double crosser, and keeps the approved clients from releasing their keys. The methodology is to give every client an unmistakable arrangement of keys, which is considered as "watermark" for following. Discernibility is additionally explored for communicated encryption in [40]. In CP-ABE scheme, secret key sarenot defined over identities. Rather, they are related with a lot of qualities. Different clients may have a similar arrangement of properties. This brings accommodation to expressive access control. In any case, given a released mystery key, it is difficult to figure out the first key proprietor in customary ABE framework. It implies that the pernicious client, who sells his mystery key, nearly has little danger of being identified. The discernibility issue in CP-ABE is considered in [13], [14], [15].1.2 Motivation and Our Contributions 1.2.1 Motivation As appeared Table 1, the capacities and qualities of the current plans [7], [8], [9], [10], [11], [12], [13], [14], [16], [17], [18], [20], [21], [22], [24], [26], [27] are looked at, and their constraints are broke down underneath. The inspiration of this work is to plan an efficient recognizable approval look framework for secure distributed storage, which defeats every one of these restrictions. (1) Inflexible approved catch phrases seek: In the safe distributed storage framework, a great deal of archives is put away in scrambled structure. It is important to give flexible secure catchphrase question capacity to encourage the archive look. Moreover, the cloud files are wanted to be shared among various information clients utilizing a flexible approval component. These two necessities ought to be at the same time supported in one system. However,the schemes in [12],[16],[17],[18],[20],[21],[22] cannot realize flexible authorization, while the plans in [9], [10], [11], [13], [14], [24], [26], [27] can't bolster catchphrase look work. In spite of the fact that the plans in [7], [8] acknowledge approved watchword seek, the catchphrase inquiry designs are not

flexible. Liang's plan [8] just considers single catchphrase seek. Sun's plan [7] bolsters conjunctive watchword look, where the query.keyword set must be actually equivalent to the separated catchphrase set from the file. On the off chance that one of the inquiry catchphrase is excluded in (or diverse from the extracted keyword set, the fileisnotre turned. They are farm or from satisfying clients' reasonable necessities. (2) Inflexible framework augmentation: Many existing approval plans [7], [8], [10], [11], [13], [24], [26], [27] are inflexible for the framework expansion. The credit set should be predefined amid the framework foundation stage, and a greatest number of the property set ought to be resolved. In the event that another credit is to be added to the framework, the whole framework must be re-built and all encoded files must be re-scrambled. It would be a debacle to the distributed storage framework. (3) Inefficient unscrambling: A primary disadvantage of numerous ABE based fine-grained get to control plans [7], [8], [13], [14], [24], [27] is that the calculation cost required for decoding develops straightly with the unpredictability of access structure. With the quick advancement of versatile terminals, (for example, cell phones), the costly.

II RELATED WORK

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 [12], which is important in protecting the privacy of outsourced data. Data owners in PEKS schemes [7], [8], [16] 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. [5] showed that PEKS schemes could be utilized to construct searchable audit logs. Later, Xu et al. [17] presented a general framework to combine PEKS and fuzzy keyword search without concrete construction. Tang [18] proposed a multiparty searchable encryption scheme together with a bilinear pairing based scheme. In 2016, Chen et al. [3] introduced the concept "dual-server" into PEKS to resist off-line keyword guessing attack. Yang et al. [19] introduced time-release and proxy reencryption method to PEKS scheme in order to realize time controlled authority delegation. Wang et al. [1] proposed a ranked keyword search scheme for searchable symmetric encryption, in which the order-preserving symmetric encryption is utilized [35]. Cao et al. [36] designed a novel system to realize multiple keywords ranked search. Searchable encryption is also further studied in [20], [21], [22].

ABE

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 cipher texts. A certain secret key can decrypt a ciphertext if and only if the associated attributes and the access policy match each other. The notion of ABE was proposed by Sahai et al. [23] 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 (CP-ABE) [24] and key-policy ABE (KP-ABE) [25]. Since the Sahai's seminal work, ABE based access control becomes a research focus [9], [10], [11], [26]. Considering the challenges in expressing access control policy, ABE scheme with non-monotonic access structure is proposed [27]. ABE systems with constant size ciphertext [28], [29] are constructed to reduce the storage overhead. In order to accelerate the decryption, researchers make effort to speed up the decryption algorithm [30], [31]. Decentralized ABE is investigated in [32][33][34], in which multiple authorities work independently without collaboration.

Traitor Tracing

Traitor tracing was introduced by Chor et al. [35]-[37] 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 [38], [39]. 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 [40]-[43]. 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[44][45]. 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 in [13], [14], [15].

Scheme	F1	F2	F3	F4	F5	F6	F7	F8	F9
[12]	×	√	×	–	×	×	×	×	×
[16]	×	√	√	–	×	×	×	×	×
[17]	×	√	×	–	×	×	×	×	×
[18]	×	√	×	–	×	×	×	×	×
[20]	×	√	×	–	×	×	×	×	×
[21]	×	√	×	–	×	×	×	×	×
[22]	×	√	×	–	×	×	×	×	×
[7]	√	√	×	×	×	×	×	√	×
[8]	√	√	×	×	×	×	×	×	×
[9]	√	×	×	√	√	×	×	×	×
[10]	√	×	×	×	√	√	×	×	×
[11]	√	×	×	×	√	√	×	×	×
[13]	√	×	×	×	×	×	√	×	×
[14]	√	×	×	√	×	×	√	×	×
[24]	√	×	×	×	×	×	×	×	×
[26]	√	×	×	×	√	√	×	×	×
[27]	√	×	×	×	×	×	×	×	×
EF-TAMKS -VOD	√	√	√	√	√	√	√	√	√

F1: fine-grained access control F2: keyword search
F3: multiple keywords subset search
F4: flexible system extension (flexible number of attributes)
F5: efficient decryption F6: verifiable decryption
F7: white-box traceability
F8: user revocation F9: key escrow free

EXISTING SYSTEM:

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 other authorized user. However, most of the available systems require the user to perform a large amount of complex bilinear pairing operations. These overwhelmed computations become a heavy burden for user's terminal, which is especially serious for energy constrained devices. 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.

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 polynomially 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

TAMKS-VOD

In order to provide an easier way to understand EF-TAMKS-VOD, we design a **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (TAMKS-VOD), where KGC is responsible to generate user's public/secret key pair like in traditional PEKS schemes. In section 4, the key escrow problem is resolved using an interactive operation between KGC and cloud server.

The system model of TAMKS-VOD is presented in Fig. 1, and the formal definition is provided in Section A in the Supplemental Materials. The system comprises of four entities, whose responsibilities and interactions are described below.

(1) **Key generation centre (KGC)**. 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.

(2) **Cloud server (CS)**. 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.

(3) **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.

(4) **Data user**. Each data user has attribute set to describe his characteristics, such as professor, computer science col-lege, 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.

Notation	Description
G/G_T	cyclic multiplicative group with prime order p
e	bilinear pairing $e : G \times G \rightarrow G_T$
Z_p^*	$\{1, 2, \cdots, p-1\}$
$[l]$	$\{1, 2, \cdots, l\}$
$\mathcal{K}$	key space
$x \in_R B$	pick an element x at random and uniformly from a finite set B
h	cryptographic hash function $h : \{0,1\}^* \rightarrow \mathcal{K}$
H	cryptographic hash function $H : \{0,1\}^* \rightarrow G$
H'	cryptographic hash function $H : \{0,1\}^* \rightarrow Z_p^*$
PK/MSK	public key/master secret key
$S/(A, \rho)$	attribute set/access structure
$PK_{id,S}/SK_{id,S}$	public key/ secret key pair of user (with identity id and attribute set S)
KW/T_{KW}	keyword set/keyword set trapdoor
CT/CT_{out}	ciphertext/transformed ciphertext
VK_M	verification key
$SEnc/SDec$ $(SEnc'/SDec')$	cryptographic secure symmetric encryption/decryption pair
$HEnc/HDec$	fully homomorphic encryption /decryption pair [45]

Architecture:

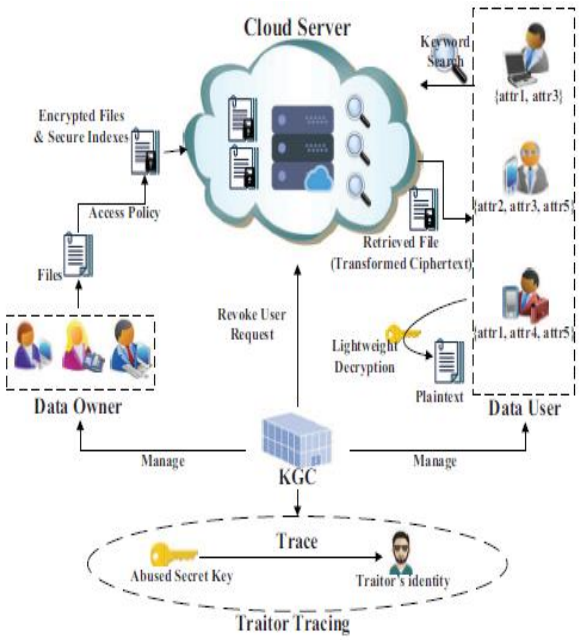


Fig: System Model

Components:

Data Owner

In this module, he logs in by using his/her user name and password. After Login the owner Uploads Data, View Files Blocks.

End User

In this module, he logs in by using his/her user name and password. After Login the user will do some operations such as Request Search Permission, Download Request, View All Files, Download File.

Fog Server

In this module, the Fog Server can do following operations such as View Files Blocks,View All Fog User Details and process the end user operations to send data block.

Cloud Server

The Cloud server as a server to provide data storage service and can also do the following operations such as View End Users and Authorize ,View Data Owners and Authorize, View All Stored Data, View Transactions ,View Attackers, View Search Request, View Download_Request, View Files Rank In Chart, View Time Delay In Chart, View Throughput In Chart.

The mail contributions in this paper are:

Flexible Authorized Keyword Search:

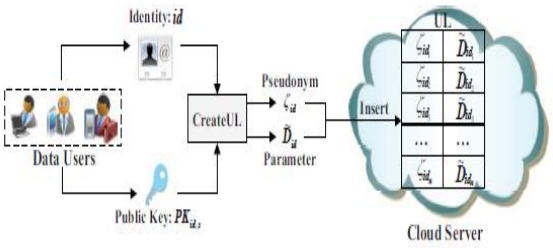
EF-TAMKSVOD achieves fine-grained data access authorization and supports multiple keyword subset search. In the encryption phase, a keyword set KW is extracted from the file, and both of KW and the file are encrypted. An access policy is also enforced to define the authorized types of users. In the search 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.

Flexible System Extension 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 polynomially 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 or storage cost is brought to EF-TAMKS-VOD. This feature is desirable for the cloud system for its ever increasing user volume.

Efficient Verifiable Decryption EF-TAMKS-VOD adopts the outsouced decryption mechanism to realize efficient decryption. Most of the decryption computation is outsourced to the cloud server, and the data user is able to complete the final decryption with an ultra lightweight computation. Moreover, the correctness of the cloud server's partial decryption computation can be verified by the user.

White-box Traceability of Abused Secret Key Traitor tracing can be divided into white-box and black-box traceability. If an authorized user leaks or sells his secret key, white-box traceability is capable to identify who leaks the key. Black-box traceability is a stronger conception, in which the leakage of a malicious user is the search and decryption equipment instead of the secret key. EF-TAMKS-VOD achieves white-box traceability. Any subscriber who leaks the secret key to a third party intentionally or unintentionally can be traced. Furthermore, the traceability of EFTAMKS-VOD does not bring additional computation and transmission overhead.

Efficient User Revocation Once a user is identified as traitor through tracing algorithm, EF-TAMKS-VOD revokes this malicious user from the authorized group. Compared with the existing scheme [7], the revocation mechanism of EF-TAMKS-VOD has much better efficiency.



Key Escrow Free In order to reduce the trust on KGC, an interactive key generation protocol is designed to solve the key escrow problem. EF-TAMKS-VOD adopts an interaction process between KGC and cloud server such that none of them is capable to independently generate the whole secret key of the user, where a lightweight homomorphic encryption algorithm is utilized. Thus, the user's secret key is not escrowed to any entity and EF-TAMKS-VOD is key escrow free.

Algorithm Implementation

Fully homomorphic encryption

A fully homomorphic encryption system enables computations to be performed on encrypted data without needing to first decrypt the data. Such cryptosystems have natural applications in secure, privacy-preserving computation as well as many other areas. Since Gentry's breakthrough work on fully homomorphic encryption (FHE), there has been much excitement and attention devoted towards developing practical FHE systems. In this project, we provide an implementation of Brakerski's scale-invariant somewhat homomorphic encryption (SWHE) system [Bra12]. In addition, we examine several candidate applications of FHE and SWHE systems, such as performing statistical analysis on encrypted data or evaluating private database queries over an encrypted database.

System Workflow

TAMKS-VOD has eight algorithms Setup, KeyGen, CreteU L, Enc, Trapdoor, Test&Transform, Dec, KeySanityCheck&T race, and the system workflow is shown in Fig. 2. In of the system establishment phase, KGC runs Setup algorithm (illustrated in Fig. 3) to generate the public parameter P P and master secret key M SK of the system. The master secret key M SK is kept secret by KGC. The sys-tem public parameter P P is disseminated to cloud server, data owners and users.

(2) For a system user (including data owner and data user) with attribute set S and identity id, KGC runs KeyGen algorithm (illustrated in Fig. 3) to generate an attribute public key P $K_{id;S}$ and secret key $SK_{id;S}$, in which the users' identity id and attribute set S are implicitly embedded. The attribute set S describes the characteristic of the user's identity id. For example, a doctor Alice of oncology department in Raffles hospital has the attribute set S_a = fdoctor, oncology department, Raffles hospitalg, and gets the attribute public/secret key pair P $K_{id;S}$=$SK_{id;S}$, where identity id ="Alice" and attribute set S = S_A.

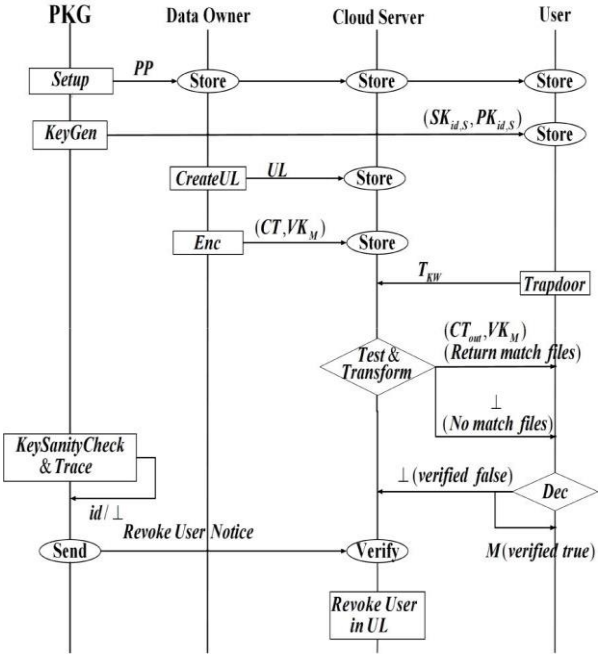


Fig: Work flow of proposed system

(3) A data user list U L is stored by the cloud server. The data owner runs CreateU L algorithm (illustrated in

Fig. 4) to generate a pseudonym $_{id}$ and a parameter~D_{id} for each authorized user with identity id. The tuple~ ($_{id}$; D_{id}) is inserted into U L, which is used in the following T est&T ransf orm algorithm and user revocation phase.

(4) The data owner runs Enc algorithm (illustrated in Fig. 5) to encrypt the file M and the extracted keyword set KW. In this process, an access policy (A;) is specified to define the set of authorized users, which is embedded into the ciphertext. Meanwhile, a verification key V K_M is gen-erated in the Enc algorithm, which is used to verify the cor-rectness of the transformed ciphertext CT_{out} that is gener-ated by the cloud server in the following T est&T ransf orm algorithm. The encrypted files, secure keyword set indexes and verification key are outsourced to cloud server.

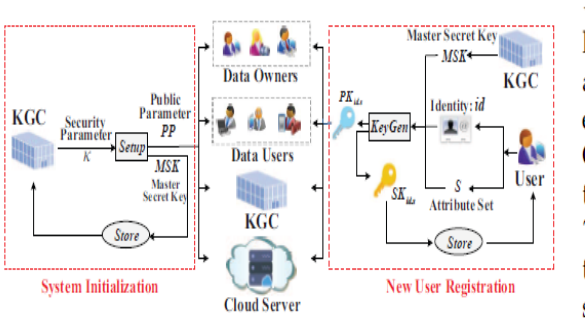
(5) In the query phase, data user specifies a query key-word set KW ^{0} and runs T rapdoor algorithm (illustrated in Fig. 6) to generate a trapdoor T_{KW} 0 using his attribute secret key $SK_{id;S}$. Data user's attribute set S is implicitly embedded into the trapdoor. Then, the data user submits T_{KW} 0 to the cloud server.

(6) Receiving the search query from the data user, the cloud server runs Test & Transform algorithm (illustrated in Fig. 7) to search on the data owner's encrypted files. The Test & Transform algorithm is divided into two algorithms, i.e., Test algorithm and Transform algorithm.

In the Test algorithm, CS tests whether the query key-word set KW^{0} (implicitly embedded in T_{KW} 0) is a subset of KW (implicitly embedded in CT) and whether the attribute set S (implicitly embedded in T_{KW} 0) satisfies the access policy (A;) (implicitly embedded in CT). If one of the two conditions does not satisfy, the Test algorithm outputs "0" and the Trasform algorithm outputs a symbol? Indicating that they do not match. If both of the two conditions satisfy, the Test algorithm outputs "1" indicate that the ciphertext CT matches with the trapdoor T_{KW} 0. Then, the Trasform algorithm outputs a transformed ciphertext CT_{out}, so that the data user can recover the plain-text M using a lightweight calculation in the following Dec algorithm. The transformed ciphertext CT_{out} and the corresponding verification key V K_M is returned to the data user.

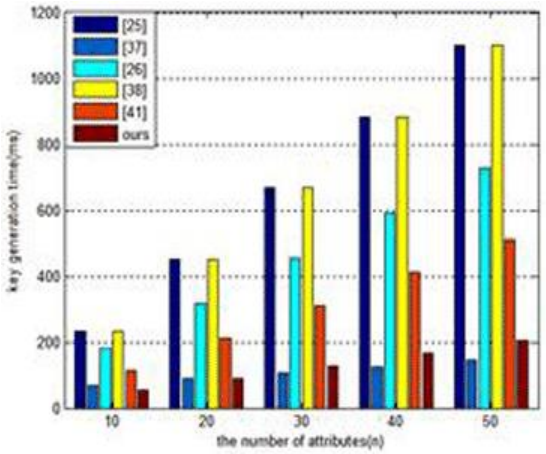
In Dec algorithm (illustrated in Fig. 8), the data user verifies whether the transformed ciphertext CT_{out} is correct using the verification key V K_M . If invalid, a symbol? is returned to cloud server. Otherwise, the data user executes lightweight computation to recover the message M.

(8) If a secret key is sold for beneficial gain, KeySanityCheck&T race algorithm (illustrated in Fig. 9) is run by KGC to check the validity of the key. If the secret key is not well-formed, KeySanityCheck algorithm outputs 0, and T race algorithm outputs a symbol?. Otherwise, KeySanityCheck algorithm outputs 1, and T race algorithm recovers the real identity of the sold secret key's owner.

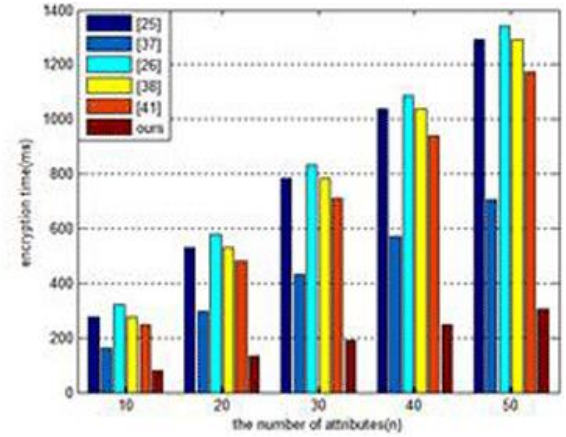


(9) After the traitor is traced, KGC sends a revocation request to CS to revoke the user.

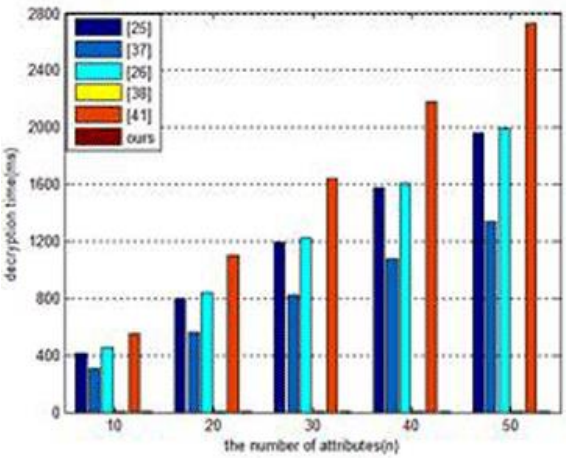
The Following graphs show the computation overheads of key generation, encryption, decryption, trapdoor generation, test and transform, and key sanity check and trace algorithms.



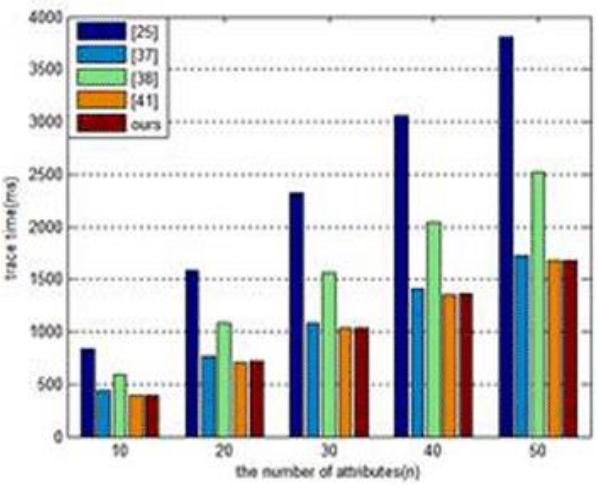
(a) Key generation time



(b) Encryption time



(c) Decryption time



(d) Trace time

V. RESULT

Publicly Verifiable ODB the present ODB schemes simply support non-public verifiability. That is, as solely {the knowledge|the info|the information} owner will check the validity of his own data as a result of solely the information owner is aware of the key. The information owner should be concerned in each verification therefore; the way to style a publically verifiable ODB theme is a remarkable downside. Privacy-preserving VDB. the normal VDB schemes don't take into account the privacy of users. Specifically, data regarding update patterns (i.e., the updated knowledge things and also the update frequency) is leaked to the CSP. A valuable analysis direction is the way to construct privacy - protective VDB theme. User - rescindable deduplication though the traceability of malicious users are often achieved in secure knowledge deduplication, the matter of user revocation still has to be addressed in multi-user situations. Thus, one valuable analysis topic is that the development of knowledge deduplication mechanism supporting user revocation.

VI. CONCLUSION

This paper focuses the enforcement of access control and the support of keyword search is important issues in secure cloud storage system. In this work, we defined 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 of users.

VII. REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, 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.Deen. "Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning," IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

[3] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server PublicKey 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. Choo, J. Weng."An efficient privacy preserving outsourced calculation toolkit with multiple keys."IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "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. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[8] 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.19811992.

[9] Green, S.Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," 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. 13431354.

[11]B.Qin, R.H.Deng, S.Liu, and S.Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced

Decryption," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in: EUROCRYPT, 2004, pp. 506-522.

[13] Z. Liu, Z. Cao, D.S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 1, pp. 76-88.

[14] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 6, pp. 1274-1288.

[15] Z. Liu, Z. Cao, D.S. Wong, "Traceable CP-ABE: how to trace decryption devices found in the wild," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

[16] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in: 4th Theory Cryptogrophy Confonference, 2007, vol. 4392, pp. 535-554.

[17] P. Xu, H. Jin, Q. Wu and W. Wang, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Schem eunder Keyword Gusssing Attack," IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277.

[18] Q. Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, 2014, vol. 9, no. 11, 1943-1952.

[19] Y. Yang and M. Ma, "Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds," IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 746-759.

[20] B. Zhang, F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.

[21] X. Wang, X. Huang, X. Yang, L. Liu, X. Wu, "Further observation on proxy re-encryption with keyword search," Journal of Systems and Software, 2012, vol. 85, no. 3, pp. 643-654.2168-7161 (c) 2018 IEEE. Personal use is permitted, but republication/ redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.14

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

[23] A. Sahai, B. Waters, "Fuzzy identity-based encryption," in: EUROCRYPT, Springer, 2005, vol. 3494, pp. 457-473.

[24] J. Han, W. Susilo, Y. Mu. "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption,"IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678.

[25] Y. Shi, Q. Zheng, J. Liu. "Directly revocable key-policy attributebased encryption with verifiable ciphertext delegation," Information Sciences, 2015, vol. 295, pp. 221-231.

[26] X.Mao, J.Lai, Q.Mei, K.Chen and J. Weng, "Generic and Efficient onstructions of Attribute-Based Encryption with Verifiable Outsourced Decryption," IEEE Transactions on Dependable and Secure Computing, publish online, DOI: 10.1109/TDSC.2015.2423669.

[27] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with nonmonotonic access structures," in: 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195203.

[28] C. Wang, J. Luo, "A key-policy attribute-based encryption scheme with constant size ciphertext," in: 8th International Conference on Computational Intelligence and Security, 2012, pp. 447-451.

[29] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," In: 5th International Conference on Provable Security, Springer, 2011, pp. 84-101.

[30] S. Hohenberger, B. Waters, "Attribute-based encryption with fast decryption," in: PKC, springer, 2013, vol. 7778, pp. 162-179.

[31] D. Nishant, J. Devesh, "Fully secure ciphertext policy attribute based encryption with constant length ciphert extand faster decryption," Security and Communication Networks, 2014, vol. 7, no. 11, pp. 1988-2002.

[32] A.Lewko and B. Waters, "Decentralizing attribute-based encryption," in CRYPTO, Springer, 2011, vol. 6632, pp. 568-588.

[33] W. Guo, J. Li, G. Chen, Y. Niu, C. Chen, "A PSO-Optimized Realtime Fault-tolerant Task Allocation Algorithm in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12), pp. 3236-3249.

[34] W. Guo, J. Chen, G. Chen, H. Zheng, "Trust Dynamic Task Allocation Algorithm with Nash Equilibrium for Heterogeneous Wireless Sensor Network," Security and Communication Networks, 2015, 8(10). pp. 1865-1877.

[35] C. Wang, N. Cao, K. Ren, W. Lou. "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on parallel and distributed systems, 2012, 23(8): 1467-1479.

[36] N. Cao, C. Wang, M. Li, K. Ren, W. Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, 2014, 25(1): 222233.

[37] B. Chor, A. Fiat, and M. Naor. "Tracing traitors". In: CRYPTO, Springer, 1994, pp. 257-270.

[38] Z. Zhou, D. Huang, and Z. Wang. "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption." IEEE Transactions on Computers, 2015, vol. 64, no.1, pp. 126138.

[39] J. Kim, W. Susilo, M. Au and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, pp. 679-693.

[40] D. Hofheinz, C. Striecks, "A generic view on trace-and-revoke broadcast encryption schemes," In: CT-RSA, Springer, 2014, pp. 4863.

[41] A. Beimel. "Secure Schemes for Secret Sharing and Key Distribution". PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[42] D. Boneh and X. Boyen, "Short signatures without random oracles," in: CRYPTO, Springer, 2004, vol. 3027, pp. 56-73.

[43] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in: PKC, Springer, 2011, vol. 6571, pp. 53-70.

[44] B. Lynn. "The Stanford Pairing Based Crypto Library." [Online]. Available: http://crypto.stanford.edu/pbc, accessed May 7, 2014.

[45] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," In: EUROCRYPT, 2010, pp. 24-43.

Authors Profile

Ms. **Chandrika Gopisetty** pursuing MCA 3rd year in Qis College and Engineering and Technology in Department of Master of Computer Applications, Ongole.

Mr. **Katti Jaya Krishna** is currently working as an Assistant Professor in Department of Master of Computer Applications in QIS College of Engineering & Technology.