JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

Privacy-Conserving Multi-Key Term Graded Search Over Encoded Rain Cloud Data

V.R.Sindhuja[1*] and K.Meena[2]

[1]M.Tech Scholar, Department of Software Engineering, PMU, Thanjavur.
[2] Asst.Prof, Department of Software Engineering, PMU, Thanjavur.
www.ijcaonline.org

Received: Dec /26/2014 Revised: Jan/8/2015 Accepted: Jan/20/2015 Published: Jan/31/2015

***Abstract*—** With the advent of rain raincloud computing, facts owners are single-minded to out groundwork their difficult facts group systems meanwhile resident spots to the profitable communal rain raincloud aimed at greon suppleness then commercial savings. Nonetheless aimed at defensive facts privacy, subtle facts has to be encoded earlier outsourcing, which obsoletes old-style facts use founded on plain manuscript key term search. Thus, permitting an encoded rain raincloud facts pursuit facility is of par quantity importance. Seeing the big digit of facts employees then papers in the cloud, it is essential to let around key influences in the pursuit appeal then homecoming papers in the order of their significance to these keywords. Related everything on search intelligent encryption attention on lone key term pursuit or Boolean key term search, then rafaith sort the pursuit results. In this paper, aimed at the chief time, we label then resolve the stimulating tricky of privacy conserving multi-key term graded pursuit over encoded rain raincloud facts (MRSE). We originate a set of severe confidentiality supplies aimed at such a safe rain raincloud facts use system. Amid numerous multicenter semantics, we select the well-prearranged corresponding quantity of "organize matching", i.e., as around cup tie as possible, to imprisonment the significance of facts papers to the pursuit query. We extra use "inner produce similarity" to quantitatively assess such corresponding measure. We chief proposal a elementary idea aimed at the MRSE founded on safe inner produce computation, then then stretch two knowingly healthier MRSE systems to attain numerous severe confidentiality supplies in two altered danger models. Thoroughgoing enquiry extra withdrawal confidentiality then productivity assurances of planned systems is given. Trials on the real dataset extra display planned systems certainly preferred low overhead advertisement on calculation then communication.

***Keywords*—**Component; Formatting; Style; Styling; Insert

I. INTRODUCTION

Rain raincloud devious is the lengthy dreamed vision of devious as a utility, currently rain cloud customers container remotely hoard their facts into the rain cloud therefore as to enjoy the on-demean tall excellence submissions then facilities meanwhile a communal pool of configure intelligent devious capitals [1]. Its greon suppleness then commercial savings are motivating together individuals then enterprises to out ground work their resident difficult facts group scheme into the cloud. To defend facts confidentiality then combon unsolicited accesses in the rain cloud then beyond, subtle data, e.g., emails, distinct fitness records, print albums, tax documents, financial transactions, etc., may have to be encoded via facts owners earlier subcontracting to the profitable communal rain cloud [2]; this, however, obsoletes the old-style facts use facility founded on plain manuscript key term search. The small answer of transferring all the facts then decrypting nearby is clinitial impractical, owing to the enormous quantity of bandwidth charge in rain cloud measure systems. Moreover, a lateral meanwhile removing the resident packing management, packing facts into the rain cloud aids no

Drive unfewer they container be just searched then utilized. Thus, discovering privacy-conserving then real pursuit facility over encoded rain cloud facts is of par quantity importance. Seeing the potentially big digit of on-demthen facts employees then enormous quantity of subcontracted facts papers in the cloud, this tricky is chiefly stimulating as it is really problematic to encounter AL therefore the supplies of performance, scheme uscapability then scalability.

On the one hand, to encounter the real facts recovery need, the big quantity of papers demthen the rain cloud waiter to per method result significance ranking, in its home of frequent indistinguishable results. Such graded pursuit scheme enables facts employees to find the most applicintelligent info quickly, somewhat than burdensomely cataloging complete all competition in the gratified group [3]. Graded pursuit container ALtherefore elegantly eradicate unessential scheme circulation via sending spinal lone the most applicintelligent data, which is really Desir intelligent in the "pay-as-youuse" rain cloud paradigm. Aimed at confidentiality protection, such location operation, however, should not leak around key term related information. On the extra hand, to expthen the pursuit result correctness as well as to demonstrate the operator exaremoval experience, it is AL therefore essential aimed at such location scheme to provision maround keyinfluences search, as lone keyterm pursuit regularly crops far too rough results. As a communal repetition selected via today's mesh pursuit machines (e.g., google search), facts employees may tfinish to deliver a set of keyinfluences in its home of lone one as the pointer of their pursuit attention to save the most applicintelligent data. Then all keyterm in the pursuit appeal is intelligent to comfort thin dindividual the pursuit result further. "organize matching" [4], i.e., as maround cup tie as possible, is an well-prearranged corresponding quantity amid such multi-keyterm semantics to refine the result relevance, then has been normally used in the plain manuscript info recovery (ir) community. However, in what way to smear it in the encoded rain cloud facts pursuit scheme remainders a very stimulating chore since of inherent refuge then confidentiality obstacles, counting numerous severe supplies comparable the facts privacy, the guide privacy, the keyterm privacy, then maround others (understthen unit iii-b).

In the literature, searchintelligent encryption [5]–[13] is a helpful method thon treats encoded facts as papers then permits a operator to secufaith pursuit complete a lone keyterm then save papers of interest. However, straight appeal of these methods to the safe big measure rain cloud facts use scheme would not be necessarily suitable, as they are established as crypto primitives then cannot accommoday of the week such tall service-level supplies comparable scheme usability, operator exaremoval experience, then inproper info discovery. Nevertheless sure new designs have been planned to provision boolean keyterm pursuit [14]–[21] as an exertion to supplement the pursuit flexibility, they are static not adequate to deliver employees with accepbench result location functionality (understthen unit vi). Our initial exertion [22] has been mindful of this problem, then if a answer to the safe graded pursuit over encoded facts tricky nonetheless lone aimed at enquiries containing of a lone keyword. In what way to idea an well-prearranged encoded facts pursuit maneuver thon ropes multi-keyterm semantics without confidentiality openings static remainders a stimulating open problem.

In this paper, aimed at the chief time, we label then resolve the tricky of multi-keyterm graded pursuit over encoded rain cloud facts (MRSE) smooth nevertheless conserving severe system-wise confidentiality in the rain cloud devious paradigm. Amid numerous multicenter semantics, we select the well-prearranged corresponding quantity of "organize matching", i.e., as around cup tie as possible, to imprisonment the significance of facts papers to the pursuit query. Specifically, we use "inner produce similarity" [4], i.e., the digit of enquiry key influences look as if in a document, to quantitatively assess such corresponding quantity of thon document to the pursuit query. Aimed at the duration of the guide construction, all document is linked with a second trail as a sub guide currently all minute regifts whether reliable key term is incomplete in the document. The pursuit enquiry is ALtherefore labelled as a second trail currently all minute earnings whether reliable key term look as if in this pursuit request, therefore the corresponding could be accurately measured via the inner produce of the enquiry trail with the facts vector. However, straight subcontracting the facts trail or the enquiry trail will violate the guide confidentiality or the pursuit privacy. To encounter the examination of supporting such multi-keyterm semantic without confidentiality breaches, we proposal a elementary idea aimed at the MRSE by safe inner produce computation, which is changed meanwhile a safe k-adjacent national (knn) method [4], then then stretch two knowingly healthier MRSE systems in a step-byststage way to attain numerous severe confidentiality supplies in two danger replicas with augmented bout capabilities. Our aids are summarized as follows,

1) Aimed at the chief time, we discover the tricky of multikeyterm graded pursuit over encoded rain cloud data, then originate a set of severe confidentiality supplies aimed at such a safe rain cloud facts use system.

2) We proposal two MRSE systems founded on the corresponding quantity of "organize matching" smooth nevertheless meeting altered confidentiality supplies in two altered danger models.

3) Thoroughgoing enquiry exawithdrawal confidentiality then productivity assurances of the planned systems is given, then trials on the real dataset extra display the planned systems certainly preferred low overheadvertisement ON calculatiON THEN communication.

THE remaindeR OF This newspaapiecE iS prearrangeD AS follows. IN Unit II, WE preferred THE SCHEME model, the danger model, our idea goals, then the preliminary. Unit iii describes The MRSE frame exertion then confidentiality requirements, shadowed via unit iv, which labels the planned schemes. Unit v gifts perfect results. We converse related exertion on together lone then Boolean key term search intelligent encryption in unit vi, then conclude the newspaapiece in unit vii.

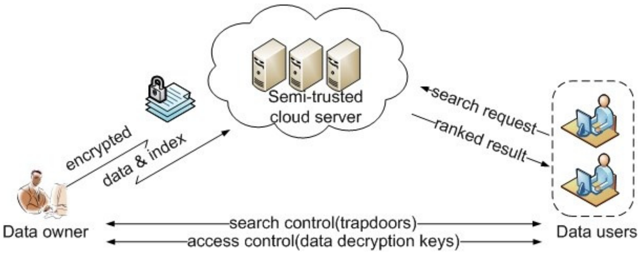


Fig. 1: building of the pursuit over encoded rain cloud data

II. TRICKY FORMULATION

A. *Scheme model*

Seeing a rain cloud facts hosting facility involving three altered entities, as confirmed in fig. 1: the facts owner, the facts user, then the rain cloud server. The facts proprietor has a group of facts papers $\mathcal{F}$ to be subcontracted to the rain cloud waiter in the encoded method ⍰. To enintelligent the exaremoval competence over ⍰ aimed at real facts utilization, the facts owner, earlier outsourcing, will chief magnitude an encoded searchintelligent guide $\mathcal{I}$ meanwhile ⍰, then then outground work together the guide $\mathcal{I}$ then the encoded document group □ to the rain cloud server. To pursuit the document group aimed at □ presumed keywords, an official operator acquires a reliable entrance □ complete pursuit switch mechanisms, e.g., transmission encryption [8]. Upon getting □ meanwhile a facts user, the rain cloud waiter is answerable to pursuit the guide $\mathcal{I}$ then homecoming the reliable set of encoded documents. To expthen the document recovery accuracy, the pursuit result should be graded via the rain cloud waiter agreeing to sure location measures (e.g., organize matching, as will be obtainable shortly). Moreover, to reduction the communication cost, the facts operator may sfinish an optional digit □ alengthy with the entrance □ therefore thon the rain cloud waiter lone directs spinal top-□ papers thon are most applicintelligent to the pursuit query. Finally, the contpresentation switch maneuver [23] is working to achieve decryption competences presumed to users.

B. Danger model

The rain cloud waiter is measured as “honest-but-curious” in our model, which is reliable with related everything on rain cloud refuge [23], [24]. Specifically, the rain cloud waiter acts in an “honest” manner then correctly trails the selected process specification. However, it is “curious” to supposture then examine facts (counting index) in its packing then communication flows established aimed at the duration of the process therefore as to study extra information. Founded on whatever info the rain cloud waiter knows, we reflect two danger replicas with altered bout competences as follows.

Individual cipher manuscript classical in this model, the rain cloud waiter is sup modeled to lone currently encoded dataset □ then search intelligent guide □, together of which are subcontracted meanwhile the facts owner.

Individual linked classical in this stronger model, the rain cloud waiter is sup modeled to possess extra info than whatever container be accessed in the individual cipher manuscript model. Such info may cover the overtone of presumed pursuit requests (trapdoors), as well as the dataset related arithmetical information. As an occasion of probable spells in this case, the rain cloud waiter could use the individual entrance info joint with document/key term incidence [25] to deduce/classify sure key influences in the query.

C. Idea goals

To unintelligent graded pursuit aimed at real use of subcontracted rain cloud facts under the aforestated model, our scheme idea should conpresently attain refuge then presentation assurances as follows.

- **multi-keyterm graded search:** to idea pursuit systems which let multi-keyterm enquiry then deliver result corresponding location aimed at real facts retrieval, in its home of frequent indistinguishable results.
- **privacy-preserving:** to stop the rain cloud waiter meanwhile knowledge extra info meanwhile the dataset then the index, then to encounter confidentiality supplies stated in unit iii-b.
- **efficiency:** overheadvertisement goalmouths on functionality then confidentiality should be attained with low communication then calculation overhead.

D. notations

- $\mathcal{F}$ – the plain manuscript document collection, meant as a set of □ facts papers $\mathcal{F} = (□_{1,2,\ldots,}□_{□})$.
- □ – the encoded document group deposited in the rain cloud server, meant as □ = $(□_{1,2,\ldots,}□_{□})$.
- □ – the dictionary, i.e., the keyterm set containing of □ keyword, meant as □ = $(□_{1,2,\ldots,}□_{□})$. · $\mathcal{I}$ – the searchintelligent guide linked with □, meant as $(□_{1,2,\ldots,}□_{□})$ currently All subguidE $□_{□}$ iS constructeD AIMED AT $□_{□}$.
- □□˜˜˜– THE subgroup of□˜□, representing□˜ $_1$THE keywords$□_2$˜ $_□$IN A pursuIt request, meant AS = (, ,...,$□_□$).

∵ □$^□_□$ —thethetrapdoorgradeD idfor$_{list}$theofsearchAll

documents^{request} according. to

their significance to .

E. Initial on organize matching

As a mixture of conjunctive pursuit then disjunctive search, “organize matching” [4] is an middle corresponding quantity which events the digit of enquiry keyinfluences look as if in the document to count the significance of thon document to the query. After employees kcurrently the expentation subgroup of the dataset to be retrieved, boolean enquiries permethod well with the exact pursuit obligation stated via the user. In rain cloud computing, however, this is not the practical case, presumed the enormous quantity of subcontracted data. Therefore, it is extra supple aimed at employees to stipulate a tilt of keyinfluences representative their attention then save the most applicintelligent papers with a abundant order.

III. Frameexertion then Confidentiality Supplies Aimed at MRSE

In this section, we label the frameexertion of multi-keyterm graded pursuit over encoded rain cloud facts (MRSE) then originate numerous severe system-wise confidentiality supplies aimed at such a safe rain cloud facts use system.

A. MRSE framework

Aimed at improper presentation, events on the facts papers are not individual in the frame exertion meanwhile the facts proprietor could just employ the old-style symmetric key cryptography to encode then then out ground work data. With attention on the guide then query, the MRSE scheme contains of four events as follows.

- setup(1^ℓ) *captivating a refuge boundary ℓ as input, the facts proprietor outputs a symmetric key as □□.*
- buildindex(□,□□) *founded on the dataset □, the facts proprietor builds a searchintelligent guide $\mathcal{I}$ which is encoded via the symmetric key □□ then then subcontracted to the rain cloud server. Afterward the guide construction, the document group container be independently encoded then outsourced.*
- trapdoor($\widetilde{\mathcal{W}}$) *with □ keyinfluences of attention in □˜ as input, this process makes a reliable entrance* . ˙ query(□ ,□,) *after the rain cloud waiter obtains a query□ request□˜ $\mathcal{I}$ as□˜(□ ˜□, □), it does the ˜graded pursuit on the˜*

□

Guide with the comfort of entrance, then lastly revenues, the graded id tilt of top-□ documents□ sorted via their □ corresponding with $\widetilde{\mathcal{W}}$.

Together pursuit switch then contpresentation switch are not in lateral the possibility of this paper. Smooth nevertheless the former is to regulate in what way official employees obtain trapdoors, the progressive is to achieve users' contpresentation to subcontracted documents.

B. Confidentiality supplies aimed at MRSE

The representative confidentiality assurance in the related literature, such as search intelligent encryption, is thon the waiter should study nothing nonetheless pursuit results. With this over-all confidentiality description, we discover then originate a set of severe confidentiality supplies accurately aimed at the MRSE framework.

As aimed at the *facts privacy*, the facts proprietor container resort to the old-style symmetric key cryptography to encode the facts earlier outsourcing, then positively stop the rain cloud waiter meanwhile prying into the subcontracted data. With admiration to the *guide privacy*, if the rain cloud waiter deduces around overtone amid keyinfluences then encoded papers meanwhile index, it may study the chief topic of a document, smooth the gratified of a small document [25]. Therefore, the searchintelligent guide should be constructed to stop the rain cloud waiter meanwhile execution such caring of overtone attack. Smooth nevertheless facts then guide confidentiality assurances are needed via avoidance in the related literature, numerous *pursuit confidentiality* supplies complicated in the enquiry process are extra difficult then problematic to tackle as follows.

Keyterm confidentiality as employees characteristically prefer to keep their pursuit meanwhile lifetime exmodeled to others comparable the rain cloud server, the most important concern is to hide whatever they are searching, i.e., the keyinfluences selected via the reliable trapdoor. Nevertheless the entrance container be produced in a cryptographic method to defend the enquiry keywords, the rain cloud waiter could do sure arithmetical enquiry over the pursuit result to product an estimate. As a caring of arithmetical information, *document incidence* (i.e., the digit of papers containing the keyword) is adequate to classify the keyterm with tall likelihood [26]. After the rain cloud waiter distinguishes sure linked info of the dataset, this keyterm expresentation info may be used to reverse-engineer the keyword.

Entrance unlink capability the entrance groawake drive should be a randomized one in its home of lifetime deterministic. In particular, the rain cloud waiter should not be intelligent to sup posture the overtone of around presumed trapdoors, e.g., to control whether the two hatches are designed via the acomparable pursuit request. Otherwise, the deterministic entrance groawake would stretch the rain cloud waiter benefit to accrue occurrences of altered pursuit requests regarding altered keyword(s), which may extra violate THE aforestated keyterm confidentiality requirement. Therefore THE important defense aimed at entrance unlinkcapability is to preferred adequate nondeterminacy into THE entrance groawake procedure.

Contpresentation Design Inlateral THE graded search, the contpresentation Design is the order OF pursuit results currently All pursuit result is A set OF papers With abundant order. Specifically, the pursuit result aimed at the enquiry keyterm set □˜ is meant AS □˜, containing of the id tilt of all papers graded Via their□significance to □˜. Then the contpresentation design is meant as $(\mathcal{F}_{\widetilde{\mathcal{W}}_1}, \mathcal{F}_{\widetilde{\mathcal{W}}_2}, \ldots)$which are the results of sequential searches.

Nevertheless a inadequate search intelligent encryption works, e.g., [17] has been planned to utilize remote info recovery (pir) method [27], to hide the contpresentation pattern, our planned systems are not considered to defend the contpresentation design aimed at the productivity concerns. This is since around pir founded method necessity "touch" the wfleabag dataset subcontracted on the waiter which is inwell-prearranged in the big measure rain cloud system.

IV. PRIVACY-CONSERVING THEN WELL-PREARRANGED MRS

To professionally attain multi-key term graded search, we proposal to employ "inner produce similarity" [4] to quantitatively assess the well-prearranged corresponding quantity "organize matching". Specifically, □□ is a second facts trail aimed at document □□ currently all minute □□[□] ∈ {0,1} resifts the presence of the reliable key term □□ in thon document, then □ is a second enquiry trail representative the key influences of attention currently all minute □[□] ∈{0,1} resifts the presence of the reliable key term □□ in the□˜ enquiry □˜. The similarity· mark of document □□ to enquiry is therefore articulated as the inner produce of their second column vectors, i.e., □□ □. Aimed at the drive of ranking, the rain cloud waiter necessity be presumed the competence to relate the corresponding of altered papers to the query. But, to preserve severe system-wise privacy, facts trail □□, enquiry trail □ then their inner produce □□ · □ should not be remodeled to the rain cloud server. In this section, we chief proposal a elementary idea aimed at the MRSE by safe inner produce computation, which is changed meanwhile a safe □-adjacent national (KNN) technique, then then display in what way to knowingly extend it to be privacy-conserving against altered danger replicas in the MRSE frame exertion in a step-by-stage manner.

A. MRSE i: privacy-conserving arrangement in knindividual ciphermanuscript model

1) safe knn computation: in the safe □-adjacent national (knn) arrangement [28], euclidean reserve amid a file finest □□ then a enquiry trail □ is used to excellent □ adjacent file records. The top-underground key is commodeled of one (□+1)minute trail as □ then two (□ + 1) × (□ + 1) invertible media as {□$_1$,□$_2$}, currently □ is the digit of fields aimed at all finest □□. First, all facts trail □□ then enquiry trail □ are lengthy to (□ + 1)-measurement trajectories as □□□ then □□, currently the (□ + 1)th measurement is set to −0.5||□^{2}□|| then 1, respectively. Besides, the enquiry trail □□ is climbed via a chance digit □ > 0 as (□□,). Then, □□□ is riven into two chance trajectories as {□□□′,□□″}, then □□ is ALtherefore riven into two chance trajectories as {□□′,□□″}.

Communication currently thon trail □ purstances as a excruciating indicator. Namely, if the □-th minute of □ is 0, □□□′[□] then □□□″[□] are set as the acomparable as □□□[□], smooth nevertheless □□ ′[□] then □□ ″[□] are set to two chance facts therefore thon their sum is equivalent to □□[□]; if the □th minute of □ is 1, the excruciating process is acomparable but thon □□□ then □□ are switched. The riven facts trail pair {□□□′,□□″} is encoded as$\{M_1^T\vec{p}_i', M_2^T\vec{p}_i''\}$, then the riven enquiry trail pair {□□ ′,□□ ″} is encoded as {□$_1$$^{-1}$□□ ′,□$_2$$^{-1}$□□ ″}. In the enquiry step, the produce of facts trail pair then enquiry trail pair, i.e., −0.5(||□□||^2−2□□·□), is serving as the pointer of euclidean reserve (||□□||^2−2□□·□+||□||^2) to excellent □ adjacent neighbors.

Without previous info of top-underground key, whichever facts trail nor enquiry vector, afterward such a order of processes, container be improved via exawithdrawal their reliable cipher text.

As the MRSE is by the inner produce corresponding in its home of the euclidean distance, we vital to do sure modifications on the facts structure to fit the MRSE framework. One method to do thon is via removing the measurement extension, the previous result vicissitudes to be the inner produce as □□□ · □. However, this arrangement is not decent sufficient aimed at our MRSE design. The chief object is thon the lone chance complicated is the measure feature □ in the entrance generation, which safeguards not deliver adequate no determinacy in the over-all arrangement as essential via the entrance unlink capability obligation as well as the key term confidentiality requirement. To deliver a extra progressive idea aimed at the MRSE, we currently deliver our MRSE i arrangement as follows.

2) MRSE i scheme: in our extra progressive design, in its home of just removing the lengthy measurement in the enquiry trail as we idea to do on the chief glance, we preserve this measurement spinterpretation process nonetheless allocate a new chance digit □ to the lengthy measurement in all enquiry vector. Such a newly additional chance is predictable to upsurge the trouble aimed at the rain cloud waiter to study the overtone amid the established trapdoors. In addition, as stated in the keyterm confidentiality requirement, chance should ALtherefore be careentirely familiar in the pursuit result to obfuscate the document incidence then diminish the chances aimed at re-

Corresponding Author: *XYZ*, emailed@gmail.com id of keywords. Introducing sure chance in the previous corresponding mark is an real method to whatever we imagine here. Extra specifically, uncomparable the chance complicated in the enquiry vector, we insert a fake keyterm into all facts trail then allocate a chance value to it. All distinct trail □□ is lengthy to (□+2)-measurement in its home of (□ + 1), currently a chance variintelligent □□ regiving the fake keyterm is deposited in the lengthy dimension. The wfleabag arrangement to attain graded pursuit with maround keyinfluences over encoded facts is as follows.

- setawake the facts proprietor casually makes a (□ + 2)-minute trail as □ then two (□+2)×(□+2) invertible media $\{\square_1,\square_2\}$. The top-underground key □□ is in the method of a 3-tuple as $\{\square,_1,\square_2\}$.
- buildindex(□,□□) the facts proprietor makes a second facts trail □□ aimed at all document □□, currently all second minute □□[□] regifts whether the reliable keyterm □□ look as if in the document □□. Subsequently, all plain manuscript subguide $\vec{D}_i$ is produced via put on measurement spinterpretation then excruciating events on □□. These events are acomparable with folks in the safe knn calculation but thon the (□ + 1)-th admission in $\vec{D}_i$ is set to a chance digit □□, then the (□ + 2)-th admission in □□□ is set to 1 aimed at the duration of the measurement extending. $\vec{D}_i$

is therefore → →$(D_i, \varepsilon_i, 1)$equivalent to. Finally, the subindex $I_i = \{M_1^T D_i', M_2^T D_i''\}$ is constructed aimed at all encrypted

Document □□.

- trapdoor(□˜) with □ keyinfluences of attention in □˜ as input, one second trail □ is produced currently all minute □[□] indicates whether □□ ∈ □˜ is true or false. □ is chief lengthy to □ + 1-measurement which is set to 1, then then climbed via a chance digit □ ≠ 0, then lastly lengthy to a (□ + 2)-measurement trail as □□ currently the previous measurement is set to anextra chance digit □. □□ is therefore equivalent to (□□,,). Afterward put on the acomparable excruciating then encoding events as above, the entrance □ ˜ is generated˜ 𝓙 as $\{\square_1^{-1}\square\square', _2^{-1}\square\square''\tilde{}\}$.

- computesquery□(□□the,,similarity) with thescorestrapdoorof each□□document, the cloud□□serveras in

Calculation 1. Wlog, we shoulder □ > 0. Afterward cataloging all scores, the rain cloud waiter revenues the top-□ graded id tilt □□~.

t

Withbrought into the enquiry trail then □□ brought into all facts vector, the previous corresponding inscriptions would be:

$$
\begin{aligned}
\square\square \cdot \square\square\tilde{} &= \{\square_1\square\square\square\square', \square_2\square\square\square\square''\}\cdot\{\square_{1-1}\square\square', \square_{2-1}\square\square''\} \\
&= \square\square\square' \cdot \square\square' + \square\square\square'' \cdot \square\square'' \\
&= \square\square\square \cdot \square\square \\
&= (\square\square, \square\square, 1) \cdot (\square\square, \square, \square) \\
&= \square(\square\square \cdot \square + \square\square) + \square. \qquad (1)
\end{aligned}
$$

COMMUNICATION THON IN THE SINGLE CASE, THE PREVIOUS MARK IS JUST $rD_i\cdot q$, WHICH PREAIDS THE MEASURE OVERTONE AIMED AT TWO ENQUIRIES ON

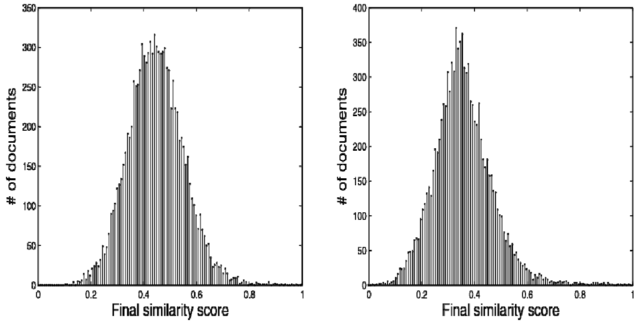


Fig. 2: delivery of previous corresponding mark with altered standard deviations, 10k documents, 10 enquiry keywords. (a) □ = 1. (b) □ = 0.5.

The acomparable keywords. Nonetheless such an topic is not at all lengthier legal in our healthier arrangement owing to the chance of together □ then □□, which clinitial validates the productivity then healthier refuge forte of our msre i mechanism.

3) analysis: we examine this MRSE i arrangement meanwhile three characteristics of idea goalmouths labelled in unit ii.

Functionality then productivity shoulder the digit of enquiry keyinfluences look as if in a document □□ is □□ = □□ · □. Meanwhile calculation 1, the previous corresponding mark as □□ = □□ · □ ˜ = (□□+□□)+□ is a lined drive of □□, currently the coefficient□□ is set as a positive chance number. However, since the chance feature ⍰$_⍰$ is obtainable as a portion of the corresponding score, the previous pursuit result on the groundwork of cataloging corresponding inscriptions may not be as exact as thon in single scheme. Aimed at the thought of pursuit accuracy, we container let ⍰$_⍰$ shadow a standard delivery (⍰,^{2}), currently the standard abnormality ⍰ purstances as a supple trade-off boundary amid pursuit correctness then security. Meanwhile the thought of effectiveness, ⍰ is predictable to be slighter therefore as to become tall exactness representative the decent cleanliness of saved documents. To quantitatively assess the pursuit accuracy, we set a quantity as exactness ⍰$_⍰$ to imprisonment the portion of returned top-⍰ papers thon are comprised in the real top-⍰ list. Thoroughgoing correctness calculation on the realworld dataset will be presumed in unit vi.

As aimed at the efficiency, our inner produce founded MRSE arrangement is an outstanding method meanwhile the presentation perspective. In the stages comparable buildguide or trapdoor, the groawake process of all subguide or entrance involves two increases of a (⍰+2)×(⍰+2) medium then a (⍰+2)-measurement vector. In the query, the previous corresponding mark is considered complete two increases of two (⍰+2)-measurement vectors.

Confidentiality as aimed at the facts privacy, old-style symmetric key encryption means could be correctly used currently then is not inlateral the possibility of this paper. The guide confidentiality is well endangered if the top-underground key SK is reserved confidential meanwhile such trail encryption method has been proved to be safe in the knindividual ciphermanuscript classical [28]. With the chance obtainable via the excruciating process then the chance facts r, then t, our bench i: $K3$ look as if in all document

Doc	Enquiry aimed at {⍰$_1$,⍰$_2$,⍰$_3$}	Query $\{K_1, K_2\}$ for $'$ r' ε t'
1	⍰$_1$ = 3,⍰$_1$ = ⍰(3+ ⍰$_1$)+ ⍰	⍰′$_1$ = 2,⍰ $_1$ = (2+ $_1$)+
2	⍰$_2$ = 2,⍰$_2$ = ⍰(2+ ⍰$_2$)+ ⍰	⍰′$_2$ = 1,⍰′$_2$ = ⍰′(1+ ⍰$_1$)+ ⍰′
3	⍰$_3$ = 1,⍰$_3$ = ⍰(1+ ⍰$_3$)+ ⍰	⍰′$_3$ = 0,⍰′$_3$ = ⍰′(0+ ⍰$_3$)+ ⍰′

Elementary arrangement container make two totally altered hatches aimed at the acomparable enquiry ⍰˜. This nondeterministic entrance groawake container assurance the *entrance unlinkcapability* which is an unresolved confidentiality leak tricky in related symmetric key founded searchintelligent encryption systems since of the deterministic stuff of entrance groawake [8]. Moreover, with correctly selected boundary ⍰ aimed at the chance feature ⍰$_⍰$, smooth the previous mark results container be obfuscated very well, averting the rain cloud waiter meanwhile knowledge the relations of presumed hatches then the reliable keywords. Communication thon nevertheless ⍰ is predictable to be minor meanwhile the productivity opinion of view, the minor one will preferred minor obfuscation into the the previous corresponding scores, which may weaken the defense of keyterm confidentiality then entrance unlinkability. As shindividual in fig. 2, the delivery of the previous corresponding inscriptions with slighter ⍰ will enintelligent the rain cloud waiter to study extra arithmetical info about the single corresponding scores, then therefore ⍰ should be set big sufficient meanwhile the thought of privacy.

B. MRSE ii: privacy-conserving arrangement in knindividual linked model

After the rain cloud waiter has info of sure linked info on the subcontracted dataset, e.g., the overtone overtone of two presumed trapdoors, sure keyterm confidentiality may not be guaranteed anyextra via the MRSE i scheme. This is probable in the knindividual linked classical since the rain cloud waiter container use measure enquiry as trails to supposture the keyterm expresentation information, e.g., document frequency, which container be extra joint with linked info to classify the keyterm in a enquiry on tall probability. Afterward giving in what way the rain cloud waiter events measure enquiry bout to disruption the keyterm privacy, we proposal a extra progressive MRSE arrangement to be privacy-conserving in the knindividual linked model.

1) measure enquiry attack: presumed two correlated hatches ⍰$_1$ then ⍰$_2$ aimed at enquiry keyinfluences {⍰$_{1,2}$} then {⍰$_1$,⍰$_2$,⍰$_3$} respectively, tcurrently will be two exceptional bags after exaremoval on around three papers as listed in tab. I then tab. Ii. In around of these two cases, tcurrently is a scheme of calculations amid previous corresponding inscriptions ⍰$_⍰$ aimed at ⍰$_1$ then ⍰′$_⍰$ aimed at ⍰$_2$ as follows,

$$\begin{cases} y_1 - y_2 = & r(1+\varepsilon_1-\varepsilon_2); \\ y'_1 - y'_2 = & r'(1+\varepsilon_1-\varepsilon_2 \\ y_2 - y_3 = & r(1+\varepsilon_2-\varepsilon_3 \\ {}' \qquad {}' & \end{cases}$$

); (2)

);

To this end, nevertheless the expresentation value of xi is encoded as yi, the rain cloud waiter could supposture thon whether all the three papers cover $K3$ or no one of them cover $K3$ complete glance the following equivalence overtone amid all bench ii: $K3$ safeguards not perform in whichever document

Doc	Enquiry aimed at {□$_1$,□$_2$,□$_3$}	Query $_{r'}$ $\{K_1, K_2\}$ $_{\varepsilon}$ for $_{t'}$
1	□$_1$ = 2,□$_1$ = □(2+ □$_1$)+ □	□′$_1$ = 2,□ $_1$ = (2+ $_1$)+
2	□$_2$ = 1,□$_2$ = □(1+ □$_2$)+ □	□′$_2$ = 1,□′$_2$ = □′(1+ □$_1$)+ □′
3	□$_3$ = 0,□$_3$ = □(0+ □$_3$)+ □	□′$_3$ = 0,□′$_3$ = □′(0+ □$_3$)+ □′

Previous corresponding inscriptions in two queries,

$$\frac{y_1 - y_2}{y'_1 - y'_2} = \frac{y_2 - y_3}{y'_2 - y'_3} = \frac{y_3 - y_1}{y'_3 - y'_1}. \qquad (3)$$

Via spinterpretation three papers to the wfleabag dataset, the rain cloud waiter could extra supposture two probable standards of document incidence of keyterm □$_3$. In the knindividual linked model, the waiter container classify the keyterm □$_3$ via referring to the keyterm expresentation document incidence info about the dataset.

2) MRSE ii scheme: the confidentiality leak shindividual overheadvertisement is produced via the protected value of chance variintelligent □$_□$ in facts trail □$_□$. To eradicate such protected stuff in around expresentation document, extra fake keyinfluences in its home of lone one should be inserted into all facts trail □$_□$. All the trajectories are lengthy to (□ + □ + 1)-measurement in its home of (□ + 2), currently □ is the digit of fake keyinfluences inserted. Healthier particulars in the MRSE ii arrangement is obtainable as follows.

- setup(1$^□$) the facts proprietor casually makes a (□ + □ +1)-minute trail as □ then two (□+□ +1)×(□+□ +1) invertible media {□$_1$,□$_2$}.

$\vec{D}_i$

- buildindex□ ∈ [1,](is□,□□set to) thea

random(□+□+1)number-th entry□$_{(□)}$in$_{\text{during}}$$^{\text{where}}$$_{\text{the}}$

Measurement extending.

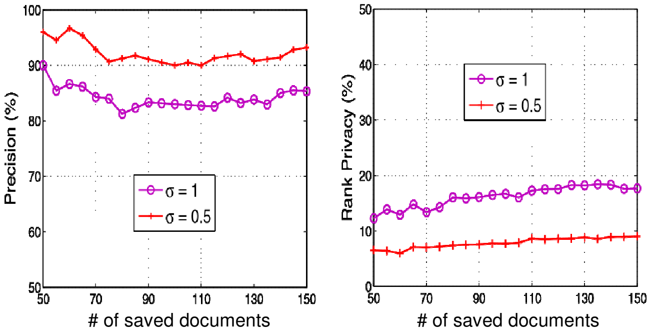
- trapdoor(□˜) via casually choosing □ out of □ fake keywords, the reliable admissions in □ are set to 1.
- query(□$_□$˜,□,□) the previous corresponding mark considered via rain cloud waiter is equivalent to $r(x_i + \sum \varepsilon_i^{(v)}) + t_i$ currently the

□-th fake keyterm is comprised in the □ selected ones.

3) *Analysis:* shoulder the likelihood of two ∑$^{(_□ □)}$ consuming the acomparable value should be fewer than 1/2$^□$, it then earnings tcurrently should be on smallest 2$^□$ altered standards of ∑□$_□$$^{(□)}$ aimed at all facts vector. The digit of altered ∑□$_{□(□)}$ is not larger than

$\binom{U}{V}$ $_U$, which is maximized after $\frac{U}{V} = 2$. Besides, considering

$\binom{U}{V} \geq (\frac{}{V})^V = 2^V$, it is better than 2$^□$ after □ = 2□ then □ = □. Therefore all facts trail should cover on smallest 2□ fake entries, then all enquiry trail will casually excellent half fake entries. Currently □ container be measured as a scheme boundary aimed at the negotiation amid productivity then privacy. With correctly location the value of □, the MRSE ii arrangement is safe against measure enquiry attack, then delivers numerous predictable confidentiality assurances inlateral the knindividual ciphermanuscript classical or the knindividual linked model. Moreover, all $^{(□)}$ is presumed to shadow the acomparable unimethod delivery (□′ − □,′ + □), currently the nasty is □′ then the alteration as □′^{2} is □^{2}/3. Agreeing to the central boundary theorem, the sum of □ self-governing chance variables □$^{(□)}$ trails the standard distribution, currently the nasty is □□′ then the alteration is □□′^{2} = □□^{2}/3. To product ∑$^{(_□ □)}$ shadow the standard distribution



(a) (b)

Fig. 3: with altered excellent of standard abnormality □ aimed at the chance variintelligent □, tcurrently is negotiation amid (a) precision, then (b) abundant privacy.

(μ,σ^2) as above, the value of μ' is set as μ/ω then the value of c is set as $\sqrt{\frac{3}{\omega}}\sigma$therefore thon $\omega\mu' = \mu$ then $\omega\sigma'^2 = \sigma^2$. With such boundary setting, pursuit correctness is statistically the Comparable as on in MRSE I scheme.

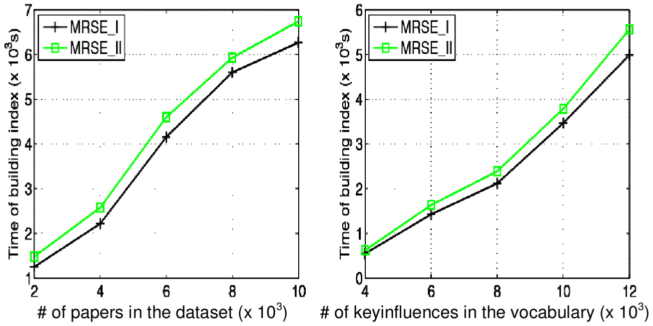
V. Presentation analysis

In this section, we demonstrate a thoroughgoing untried calculation of the planned method on a real dataset: the enron email dataset [29]. We casually excellent altered digit of emails to magnitude dataset. The wfleabag research scheme is practical via c linguistic on a linux waiter with intel xeon processor 2.93ghz. The communal helpfulness routines via numerical recipes are working to compute the inverse of matrix. The presentation of our method is assessed regarding the productivity of two planned MRSE schemes, as well as the negotiation amid pursuit exactness then privacy.

A. *Exactness then privacy*

As obtainable in unit iv, fake keyinfluences are inserted into all facts trail then sure of them are selected in all query. Therefore, corresponding inscriptions of papers will be not accurately accurate. In extra words, after the rain cloud waiter revenues top-□ papers founded on corresponding inscriptions of facts trajectories to enquiry vector, sure of real top-□ applicintelligent papers aimed at the enquiry may be excluded. This is since whichever their single corresponding inscriptions are decreased or the corresponding inscriptions of sure papers out of the real top-□ are increased, together of which are owing to the imppresentation of fake keyinfluences inserted into facts vectors. To assess the cleanliness of the □ papers saved via user, we label a quantity as exactness □□ = □′/□ currently □′ is digit of real top-□ papers thon are returned via the rain cloud server. Fig. 3(a) displays thon the exactness in MRSE arrangement is evidently pretentious via the standard abnormality □ of the chance variintelligent □. Meanwhile the thought of effectiveness, standard abnormality □ is predictable to be slighter therefore as to become tall exactness representative the decent cleanliness of saved documents.

However, user's abundant confidentiality may have been partially leaked to the rain cloud waiter as a conorder of minor □. As described



(a) (b)

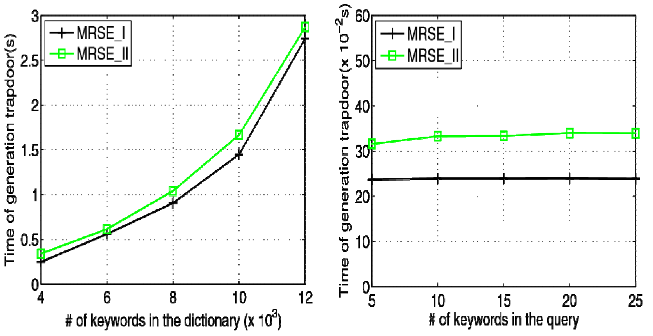
Fig. 4: retro charge of structure index. (a) aimed at the altered possibility of dataset with the comparable dictionary, n = 4000. (b) Aimed at the comparable dataset with altered possibility of dictionary, m = 1000.

In unit III-B, THE contPresentation Design is well-defined as the order OF graded pursuit results. Nevertheless pursuit results cannot be endangered (excluding luxurious pir technique), we Container static hide the abundant order OF saved papers AS ample as possible. in order to assess This confidentiality guarantee, we chief label THE abundant perturbation AS □~□ = |□□−□′□|, currently □□ is the abundant digit of document □ in the saved top-□ papers then □′□ is Its abundant digit in the real top-□ graded documents. the over-all abundant confidentiality quantity On opinion □ iS then well-defined as the regular of all the □□ aimed at all document □ in the saved top-□ documents, denoted˜ as □~□ = ∑□~□/□. Fig. 3(b) displays the abundant confidentiality on altered opinions with two standard abnormalities □ = 1 THEN □ = 0.5 respectively.

meanwhile these two figures, we container understate thon minor □ leads to progressive exactness of pursuit result Nonetheless lesser abundant confidentiality guarantee, Smooth Nevertheless big □ results in progressive abundant confidentiality assurance nonetheless lesser precision. In extra words, Our arrangement delivers A balance boundary aimed at facts employees to gratify their altered supplies on exactness then abundant privacy.

B. *Efficiency*

Guide construction: to magnitude a search intelligent sub guide □□ aimed at all document □□ in the dataset □, the chief stage is to map the key term set removed meanwhile the document □□ to a facts trail □□, shadowed via encoding all facts vector. The retro charge of charting or encoding be contingent straight on the dimensionality of facts trail which is strong-minded via the possibility of the dictionary, i.e., the digit of indexed keywords. Then the retro charge of structure the wfleabag guide is AL therefore related to the digit of sub guide which is equivalent to the digit of papers in the dataset. Fig. 4(a) displays that, presumed the comparable vocabulary currently |□| = 4000, the retro charge of structure the wfleabag guide is ninitial lined with the possibility of dataset meanwhile the retro charge of structure all subguide is fixed. Fig. 4(b) displays thon the digit of keyinfluences indexed in the vocabulary determines the retro charge of structure a subindex. As obtainable in the unit iv-a, the chief calculation to make a subguide in MRSE i contains the excruciating process then two increases of a (□ + 2) × (□ + 2) medium then a (□ + 2)-



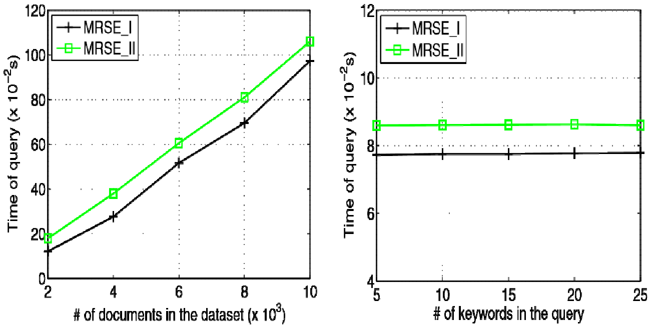
(a) (b)

Fig. 5: retro charge of manufacture trapdoor. (a) aimed at the comparable enquiry keyinfluences in lateral altered dimensions of dictionary, t = 10. (b) aimed at altered facts of enquiry keyinfluences in lateral the comparable dictionary, n = 4000.

Measurement trail currently n = |⍰|, together of which have straight overtone with the possibility of dictionary. The dimensionality of media in MRSE ii is (⍰ + ⍰ + 1) × (⍰ + ⍰ + 1) which is bigger than thon in MRSE i therefore thon the guide structure retro develops larger as individual in together fig. 4(a) then fig. 4(b). Nevertheless the retro of structure guide is not a negligible overhead advertisement aimed at the facts owner, this is a one-retro process earlier facts outsourcing. Besides, tab. Iii lists the packing overhead advertisement of all sub guide in two MRSE systems in lateral altered dimensions of dictionary. The possibility of sub guide is absolutely lined with the dimensionality of facts trail which is strong-minded via the digit of keyinfluences in the dictionary. The dimensions of sub guide are very close by in the two MRSE systems since of small changes in the dimensionality of facts vector.

*1) **Entrance generation:*** fig. 5(a) displays thon the retro to make a entrance is importantly pretentious via the digit of keyinfluences in the dictionary. Comparable guide construction, all entrance reawake incurs two increases of a medium then a riven enquiry vector, currently the dimensionality of medium or enquiry trail is altered in two planned systems then develops larger with the cumulative possibility of dictionary. Fig. 5(b) validates the entrance groawake charge in the MRSE ii arrangement is about 20 percentages larger than thon in the MRSE i scheme. Comparable the subguide generation, the alteration of prices to make hatches is majorally produced via the altered dimensionality of trail then media in the two MRSE schemes. Extra importantly, it displays thon the digit of enquiry keyinfluences has minute influence on the overheadvertisement of entrance generation, which is a important benefit over related everything on multi-keyterm searchintelligent encryption.

Query: enquiry execution in the rain cloud waiter contains of devious then location corresponding inscriptions aimed at all papers in the dataset. Fig. 6 displays the enquiry retro is dominated via the digit of papers in the dataset smooth nevertheless the digit of keyinfluences in the enquiry has very slight imppresentation on it comparable the charge of entrance groawake above. With admiration to the communication charge in query, the possibility of the entrance is



(a) **(b)**

FIG. 6: RETRO CHARGE OF QUERY. (A) AIMED AT THE ACOMPARABLE ENQUIRY KEYINFLUENCES IN ALTERED DIMENSIONS OF DATASET, T = 10. (B) AIMED AT ALTERED FACTS OF ENQUIRY KEYINFLUENCES IN THE ACOMPARABLE DATASET, M = 1000

Bench iii: possibility of subindex/trapdoor

Possibility of dictionary	4000	6000	8000	10000	12000
MRSE i (kb)	31.3	46.9	62.5	78.1	93.8
MRSE ii (kb)	32.5	48.1	63.8	79.4	95.0

The acomparable as thon of the subguide listed in the tab. Iii, which keeps continuous presumed the acomparable dictionary, not at all material in what way maround keyinfluences are incomplete in a query. Smooth nevertheless the calculation then communication charge in the enquiry process is lined with the digit of enquiry keyinfluences in extra multiple-keyterm pursuit systems [14], [16], our planned systems preferred initial continuous overhead advertisement smooth nevertheless cumulative the digit of enquiry keywords.

VI. Related work

A. *Lone keyterm search intelligent encryption*

Old-style lone key term search intelligent encryption systems [5]–[13], [22] characteristically magnitude an encoded search intelligent guide such thon its gratified is covered to the waiter newer it is presumed appropriate hatches produced complete top-underground key(s) [2]. It is chief deliberate via song et al. [5] in the symmetric key setting, then improvements then progressive refuge definitions are presumed in goh [6], chang et al. [7] then curtmola et al. [8]. Our initial exertion [22] solves safe graded keyterm pursuit which exploits key term incidence to abundant results in its home of frequent indistinguishable results. However, it lone ropes lone key term search. In the communal key setting, boneh et al. [9] preferred the chief search intelligent encryption construction, currently anyone with communal key container carve to the facts deposited on waiter nonetheless lone official employees with remote key container search. Communal key keys are characteristically very computationally luxurious however. Furthermore, the key term confidentiality could not be endangered in the communal key location meanwhile waiter could encode around key term with communal key then then use the established entrance to assess this cipher text.

B. Boolean key term search intelligent encryption

To supplement pursuit functionalities, conjunctive key term pursuit [14]–[18] over encoded facts have been proposed.

These systems incur big overhead advertisement produced via their important primitives, such as calculation charge via bylined map, e.g. [16], or communication charge via top-underground sharing, e.g. [15]. As a extra over-all pursuit approach, establish encryption systems [19]–[21] are lately planned to provision together conjunctive then disjunctive search. Conjunctive key term pursuit revenues "all-or-nothing", which earnings it lone revenues folks papers in which all the keyinfluences stated via the pursuit enquiry appear; disjunctive key term pursuit revenues indistinguishable results, which earnings it revenues all document thon covers a subgroup of the representation keywords, smooth lone one key term of interest. In short, no one of preferred Boolean key term search intelligent encryption systems provision around keyinfluences graded pursuit over encoded rain cloud facts smooth nevertheless conserving confidentiality as we proposal to discover in this paper. Communication that, inner produce enquiries in establish encryption lone predicates whether two trajectories are orthogonal or not, i.e., the inner produce value is covered but after it equals zero. Without if the competence to relate covered inner products, establish encryption is not qualified aimed at execution graded search. Furthermore, most of these systems are constructed upon the luxurious calculation of pairing events on elliptic curves. Such in productivity disbenefit AL therefore limits their practical presentation after positioned in the cloud. On a altered front, the pursuit on top-□ recovery [26] in file communal is AL therefore loosely related to our problem.

V. Conclusion

In this paper, aimed at the chief retro we label then resolve the tricky of multi-keyterm graded pursuit over encoded rain cloud data, then originate a change of confidentiality requirements. Amid numerous multi-keyterm semantics, we select the well-prearranged corresponding quantity of "organize matching", i.e., as maround cup tie as possible, to professionally imprisonment the significance of subcontracted papers to the enquiry keywords, then use "inner produce similarity" to quantitatively assess such corresponding measure. Aimed at meeting the examination of supporting multi-keyterm semantic without confidentiality breaches, we proposal a elementary idea of MRSE by safe inner produce computation. Then we stretch two knowingly healthier MRSE systems to attain numerous severe confidentiality supplies in two altered danger models. Thoroughgoing enquiry exawithdrawal confidentiality then productivity assurances of planned systems is given, then trials on the real dataset display our planned systems preferred low overheadvertisement on together calculation then communication.

As our upcoming work, we will discover supporting extra multikeyterm semantics (e.g., weighted query) over encoded data, integrity checkered of abundant order in pursuit result then confidentiality assurances in the extra stronger danger model.

REFERENCES:

[1] Zewdie, B. ; Dept. of Comput. Sci., Illinois Inst. of Technol., Chicago, IL ; Carlson, C.R. "Adaptive Component Paradigm for Highly Configurable Business Components", Published in: Electro/information Technology, 2006 IEEE International Conference on Date of Conference: 7-10 May 2006 Page(s): 185 – 190.

[2] Geisterfer, C.J.M. ; Dept. of Comput. Sci., Colorado State Univ., USA ; Ghosh, S. "Software component specification: a study in perspective of component selection and reuse" , Published in: Commercial-off-the-Shelf (COTS)-Based Software Systems, 2006. Fifth International Conference on Date of Conference: 13-16 Feb. 2006.

[3] Hamlet, D. ; Portland State Univ., OR, USA ; Mason, D. ; Woitm, D. "Theory of software reliability based on components" , Published in: Software Engineering, 2001. ICSE 2001. Proceedings of the 23rd International Conference on Date of Conference: 12-19 May 2001 Page(s): 361 – 370.

[4] Jianguo Chen ; Coll. of Inf. Eng., China Jiliang Univ., Hangzhou, China ; Yeap, W.K. ; Bruda, S.D. "A Review of Component Coupling Metrics for Component-Based Development" , Published in: Software Engineering, 2009. WCSE '09. WRI World Congress on (Volume:4) Date of Conference: 19-21 May 2009 Page(s): 65 – 69.

[5] Yong Peng ; Sch. of Mechatron. Eng. & Autom., Nat. Univ. of Defense Technol., Changsha, China ; Chunguang Peng ; Jian Huang ; Kedi Huang "An Ontology-Driven Paradigm for Component Representation and Retrieval" , Published in: Computer and Information Technology, 2009. CIT '09. Ninth IEEE International Conference on (Volume:2) Date of Conference: 11-14 Oct. 2009 Page(s): 187 – 192.

[6] Kim, L. ; Dept. of English, Memphis State Univ., TN, USA ; Albers, M.J. "Presenting information on the small-screen interface: effects of table formatting" , Published in: Professional Communication, IEEE Transactions on (Volume:46 , Issue: 2) Page(s): 94 – 104.

[7] Chamberlin, D.D. ; IBM Almaden Research Center, 650 Harry Road, San Jose, California 95120, USA "Document convergence in an interactive formatting system", Published in: IBM Journal of Research and Development (Volume:31 , Issue: 1) Page(s): 58 – 72.

[8] Stoica, Petre ; Dept. of Syst. & Control, Inf. Technol., Uppsala Univ., Sweden ; Ganesan, G. "Maximum-SNR spatial-temporal formatting designs for MIMO channels", Published in: Signal Processing, IEEE Transactions on (Volume:50 , Issue: 12) Page(s): 3036 – 3042.

[9] Linfoot, S.L. ; Founder & CTO of MediaTag Ltd., Leicester, UK ; Coughlin, T. "A cross-standard metadata formatting structure" , Published in: Consumer Electronics, IEEE Transactions on (Volume:59 , Issue: 3) Page(s): 550 – 555.

[10] Elias, S. ; Sri Venkateswara Coll. of Eng., Chennai, India ; Mathew, L. ; Easwarakumar, K.S. ; Chbeir, R. "Automatic Temporal Formatting of Multimedia Presentations Using Dynamic Petri Nets" ,Published in: Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on Date of Conference: 3-6 Aug. 2009 Page(s): 1 – 6.

[11] Dinh, Duc V. ; Institute of Solid State Physics, Technische Universität Berlin, Hardenbergstraße 36, 10623 Berlin, Germany ; Skuridina, D. ; Solopow, S. ; Frentrup, M. "Growth and characterizations of semipolar (1122) InN" , Published in: Journal of Applied Physics (Volume:112 , Issue: 1) Page(s): 013530 - 013530-9.

[12] Sarkar, P. ; Palo Alto Res. Center, CA, USA ; Nagy, G. "Style consistent classification of isogenous patterns", Published in: Pattern Analysis and Machine Intelligence, IEEE Transactions on (Volume:27 , Issue: 1) Page(s): 88 – 98.

[13] Kanagawa, H. ; Interdiscipl. Grad. Sch. of Sci. & Eng., Tokyo Inst. of Technol., Tokyo, Japan ; Nose, T. ; Kobayashi, T. "Speaker-independent style conversion for HMM-based expressive speech synthesis", Published in: Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on Date of Conference: 26-31 May 2013 Page(s): 7864 – 7868.

[14] Yu Wu ; Sch. of Journalism, Zhongnan Univ. of Econ. & Law, Wuhan, China "Research of the style computational model for Ming-style learning system", Published in: Networking and Digital Society (ICNDS), 2010 2nd International Conference on (Volume:2) Date of Conference: 30-31 May 2010 Page(s): 484 – 487.

[15] Hussein, A.M. ; Electr. & Comput. Eng. Dept., Ryerson Univ., Toronto, ON, Canada ; Milewski, M. "CN tower lightning flash components" , Published in: Lightning Protection (XI SIPDA), 2011 International Symposium on Date of Conference: 3-7 Oct. 2011 Page(s): 7 – 13.

[16] Campos, A. ; UNINOVA, Caparica ; Pina, P. ; Neves-Silva, R." Supporting Distributed Collaborative Work in Manufacturing Industry" , Published in: Collaborative Computing: Networking, Applications and Worksharing, 2006. CollaborateCom 2006. International Conference on Date of Conference: 17-20 Nov. 2006 Page(s): 1 – 6.

[17] Toma, S.-A. ; Mil. Tech. Acad., Bucharest, Romania ; Birsan, T. ; Totir, F. ; Oancea, E. "On letter to sound conversion for Romanian: A comparison of five algorithms", Published in: Speech Technology and Human - Computer Dialogue (SpeD), 2013 7th Conference on Date of Conference: 16-19 Oct. 2013 Page(s): 1 – 6.

[18] Hui Yuan ; Dept. of Educ., Sichuan Radio & TV Univ., Chengdu, China ; Sihua Zhao ; Yongmin Jiang "Trajectory planning based on physical parametric design" , Published in: Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on Date of Conference: 16-18 April 2010 Page(s): 292 – 296.

[19] Clement, G.T. ; Focused Ultrasound Lab., Harvard Med. Sch. & Brigham & Women"s Hosp., Boston, MA "Nonlinear planar forward and backward projection" , Published in: Ultrasonics Symposium, 2008. IUS 2008. IEEE Date of Conference: 2-5 Nov. 2008 Page(s): 1800 – 1803.

[20] Wei-Zhan Hung ; Dept. of Int. Businesss, Nat. ChiNan Univ., NanTou, Taiwan "Social behavior algorithm", Published in: Fuzzy Theory and it's Applications (iFUZZY), 2012 International Conference on Date of Conference: 16-18 Nov. 2012 Page(s): 57 – 61.