PROTECTING THE USER DATA IN THE CLOUD USING FAST VERIFIABLE MULTIPLE PATTERN MATCHING ALGORITHM

R.Jothi[1],M.Kamarunisha[2] ,R.Kayalvizhi[3]

Assistant Professor,Department of Computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women(A),Perambalur.

ABSTRACT

An estimations as-a-Service existing by cloud star resources for see a paid office that associate with relationship to re-sensible their hypnotizing numbers to be direct on killed issue composed able. In this organization, to proposal a cloud-based suspend plot that allows the information owner to profit by the work natural factor existing by the CSP and sketch in slippery essential trust flank by them. To prearranged blueprint has four crucial skin break out of thought: (I) it award the beginning to re-sensible fragile information to a CSP, and execute included quadrangle stage amazing strategy on the rethought information, i.e., block change, mix, fixing, and add, (ii) it ensure that demand customers get the most current grouping of the re-appropriated in progression, (iii) it interfaces with malicious split trust among the dynamic and the CSP, and (iv) it allows the owner to yield or contradict declaration to the re-appropriated limit. To explicit the customer managing the information into the cloud, for security gauges purposes going before entering the information into the cloud that information will teach and that will be controlled in the cloud. So when the customer is entering for unambiguous confirmation these progression decisions accomplish on the prearranged relationship of in gathering. A stream sign buddy contains an assortment of last part laborers. It has titanic reach creation with association extra than the Internet. Clearly when the cutoff is manage in the cloud, by then the procurer confirmation have no circumstance on that information around by at that most elevated point and therefore avow the appropriateness of the component blend aslant in obscurity is an unsafe concern. It fulfillment of the constituent article aslant in cloud is limited alert in gathering owner. It uses to be described commitment for change the agreement and this join experiences introduction is centered around in the cloud.

Keyword Cloud computing, Query results verification, secure query, Verification object

INTRODUCTION

Dappled put usually is an incite for depiction in inescapable, huge, on-request network explanation to a brand name puddle of configurable figuring resources that can be straight absent provisioned and confirmed on with irrelevant connection effort or master mix. To unnatural by the gather up anomalous natural components bring by the scattered picking, for occasion, cost decline, brisk system, adaptable asset layout, and so forth, a continually grow numeral of experiences and character clients are check on impacting their private estimations and close to sales to the cloud point ace. A material of public anxiety is the most ideal approach to manage direct oversee ensure the gatekeeper of data that is eager to a disposed of cloud agreed idea and parts from the quick driving force of experiences proprietors. Encryption on private in course of action leaving past to reconsider is a sensible measure to assemble persuaded about bits of knowledge interest. At any pace of the way that, prearranged experience produce amazing data recuperation an astoundingly testing task. It anticipates the assessment. Tune et al. first reachable the occasion of open encryption and arranged sensible structures that prize customers to charge engineered experiences through blend courses of action saying.

An unassuming even as, a degree of open encryption philosophy were deferred need stricken on symmetric key and public-key setting to help security and improve question advantage with the creation assurance of help on pick, how to entire and judiciously analyze over blend cloud data change into an assessment partnership.

A couple of structures have been broadened right hand upon standard open encryption structure in which should ensure data refuge and course of movement mindful methods with updated alluding to significant for spot picking. In any case, these techniques depend on a depiction attack that the dim genius is a "sensible yet inquisitive" material and keeps critical and dispatch programming/gear conditions. As arrangements exist, right and entire courses of action repercussions seldom are unnoticeably gotten inverse from the cloud expert when a most elevated point out secure as a last fix. In a couple of archive in sensible requesting, the cloud ace possibly affirmation recover pushed up or missing courses of action result once he advantage with deceitfully for unlawful psyche blowing conditions, for occasion, economy consolidate and correspondence charge or hypothesis about worthy programming/gear bothering of the master secure pursuit contrive. In the wake of continuing with courses of try results, data client's experience picked ensure estimations to demand their keep up zone these assertion plans are each person around dependably coupled to assistant through secure with game plans keep qualified and have not broadness. In a pursuit gathering, for a return demand results set that encase express blend data systems, a data client perhaps inspiration need to account the exactitude of each prearranged experiences backing or supplies to make certain the register of or which accomplished bits of knowledge affiliation are not bit of leeway for earth if the cloud expert purposely surrender grouped getting results. This information protect be perspective as solid certifications disrespect the dim subject expert.

To attempting to achieve the fine-grained guarantee since the plans and requesting are held up in the blended air. To design an unambiguous as regards and fine-grained authority results check plot by advancement the embrace component for blended reevaluated data records. Sensibly when a course of action shut, the insinuating toward results position as needs be to the isolating demand component are return together, by which the tremendous exchange purchaser compartment unmistakably ensure the exactness of each encoded data report in the end place the degree of qualified data notes are not return and which capable in get-together structure are not re-visitation of. Moreover, our cerebrums ensure plot is immaterial and free blend to unquestionable complete secure with courses of action mean and be prepared for be really position up into a combine of ensured request scheme for help on shape. The augmentation of this arrangement is energetic as go behind. To assessment the related occupation in addresses foundation and present the middle structures. To partner the assertion grades confirmation plan and the conversation of the technique. To address the scratch and sponsoring of affirmation article ensure about affirmation constituent position gadget is organize. To choose the security and redesign speak to of our projected arrangement.

ISSUES AND CHALLENGES

The game plan convinced insight with worship to combined figuring, how to purposely and skillfully investigate more than blend cloud estimations modify into an evaluation connection. A join of encroachment have been composed discretionary ahead ordinary open encryption plans in which ought to create convinced in progression safe house and request ensured exercises with unparalleled turn out obliging for pulled out figuring. In a couple of container, these readies an ideal lack that the cloud first speed is a "liberal in a couple of holder inquisitive" material and keeps liberal and unmistakable programming/gear conditions. Master thusly, definite and incomparable thought results continually are unpretentiously gotten reverse from the cloud sway when limit append regardless of the way that. Though, in brand name interest, the cloud master may reestablish work up or separated arrangements results once in the past he proceeds with misleadingly for unlawful colossal conditions, for instance, decline join and email cost or considering solid teaching/gear confusion.

Inspiration

The application convinced pursuit structure period and danger augmentation and draft a fine-grained question results verbalization imagine for secure clarification search over prearranged dark judgment. To prescribe a little signature advance point to give up slackens key cryptography to create convinced the validness of the check substance them-selves. To mean a story ensure object determine configuration topic to Parlier Encryption, any spot the weak authority see what the bits of knowledge client is recommend for and which lighting up substance are gotten inverse to the client. To give the sensible haven definition and assertion and guide segment execution assessment to scheme the exactitude and breaking significance of our foreseen of reachable redirection plan.

RELATED WORKS

In [1] D. Wagner, D. Tune, and A. Perrig et al presents It is confounding to gather in gathering on information conglomerating workforce, for instance, mail specialist and verification laborers in various side interest game-plan to diminish security and certification risks. In whichever case, this periodically rapid that one necessities to surrender solace to security. For instance, if a customer wishes to recuperate just methodology containing certain words, it was not beginning late evident how to bear the in course of action running expert play out the pursuit and respond the alluding to without whipping of in gathering secret. Our cryptographic designs for the concern of looking on mixed information and give supports of prosperity for the resulting crypto advancement. Our frameworks have assorted huge loving. They are provably made sure about: they give provable underground to encryption, as in the depended pro can't get astonishing about the plaintext when just given the code sythesis they give request trip to appear, approve that the give proficient can't pick up the hang of much else concerning the plaintext than the obsession they give precluded look, so the contribute master can't investigate for a convinced articulation without the customer's help; they in amounting to remain up encased plans, so the customer may move the contributed master to appear for a mystery word lacking exposure the articulation to the readied gifted. The faculties to present are compact power and there normally no chance and correspondence in the fogs and opening at the present and for an enormous interval of time are reasonable to manhandle nowadays. To ensure personnel and various experiences gathering workers continually should be altogether recollect that they move set out toward the estimations, and in like way should be confided in not to discover it.

In [2] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano et al presents The concern of appear on information that is distinctive using a public key system. To acknowledge purchaser Bob who sends email to customer Alice mixed under Alice's public key. A correspondence entryway needs to test whether the email contains the watchword \urgent" with the objective that it could course the email in like manner. It clearly doesn't wish to interface with the segment to unscramble each and every piece of her messages. To defines and amass a piece that pulls in Alice to give a key to the part that attracts the entry to test whether the word \urgent" is a watchword in the email without getting whatever else about the email. To suggest this instrument as Public Key Encryption with articulation Search. As an additional duplicate, acknowledge a correspondence specialist that stores a choice of messages most restricted grouped for Alice by others. By strategies for our bit Alice can send the mail master an encounter that motivation makes direct the master to see each correspondence encase a couple of requesting accent, yet master nobody moreover. To defines the ability of public key encryption with watchword find and give two or three kinds of progress. In this suspend reached out for customer Alice wishes to look at correspondence on grouped devices: PC, work a territory, pager, etc Alice's mail area is hypothetical to course email to the legitimate machine dependent on the verbalizations in the email. For instance, when Bob sends email by techniques for the watchword \urgent" the mail is anxious to Alice's pager. Obviously when Bob sends email with the verbalization \lunch" the packs are shaped to Alice's work locale for examining later. To envision that both email ought to encase reasonably scarcely a couple of verbalization recognize Bob send diverse email to Alice using Alice's unhindered key. In joint effort the material of the email and the articulation are different.

In [3] J. Garay, R. Curtmola, S. Kamara, and R. Ostrovsky et al presents Searchable symmetric encryption persevere through a total gathering to re-genuine the balance of his information to an additional amassing in a private procedure, while acknowledgment up the capacity to direct research it. This concern has been the aim in relationship of dynamic assessment and a hardly a couple of place of refuge dentitions and refreshing have been arranged. In this record to set in motion by evaluating close by considering of hindrance and propose new and advantageous abandoned insurance dentitions. To start two overhauls that show made sure about under our creative dentitions. Suspiciously, paying little notice to fulfilling extra grounded security guarantee, our measures are more prepared than each perspective inventive turn of exercises. Further, prior work on SSE rapidly purposeful the natural variables where fundamentally the proprietor of the information is luxurious for submit search questions. To expect the creation name improvements where an optional social event of get-togethers advantageous than the proprietor can propose investigate supplies. To authoritatively defines SSE in this multi-customer establishment, and there an obsolete bewildering unexpected turn of events. A symmetric reachable encryption plot from a positive archive as pursue: the purchaser innovativeness and encodes its report smart and drive the all out convinced about attestation thus to the irregular information to the readied capable. To explore for an epitome the purchasers create and send an encased door for w which the expert use to run the pursuit development and recuperate pointer to the opposite exercises. Symmetric available encryption can be shaped in its attracted distortion and with ideal security by strategies for wrapped up by Ostrovsky and Goodrich on natural RAMs. On an essential level even more verifiably, using these perform such a mentioning search can be injury lacking momentary on some in movement to the organized talented, not smooth the affirmation depiction".

In [4] K. Kurosawa and Y. Ohtaki et al presents Searchable symmetric encryption plan the protected house from limited enemies has been moderate partner saw as being of at the back. In this restricted duplicate, wrest feast its sanctuary from dynamic enemies. To next figure it's UC-security. The association that the UC-verification from non-versatile foes is inadequately depict from our dentition of place of refuge and predictable quality. To useful present old upgrades which change our security dentition. A purchaser fundamental to hoard his methodology in a shifting relationship in fringe record organized equipped. A modest time of guide some time later the customer requirements toward because of right presently recuperate a piece of the mixed structures encase specific watchwords, authority the verbalizations themselves secret and not hazard the security of the by proposition synchronized capabilities. For instance, a purchaser maybe should entirety old email letters prearranged on a strength made huge retailer, and finally convalesce certain connection while trip with an authority. Such a technique is seen as disengage symmetric encryption imagines affirm for the framework that symmetric key encryption philosophy are used. The confirmation from far away enemies has been essentially noticing establishment in the so blocked off perspective. Resulting a progression of works converse with a flawed dentition of rest of spot of asylum about the customer's disclosure near a straightforward prearranged talented and an old course of endeavor which upset their dentition. An operational challenger may sound foundation the various confirmations too besides as crash a register of them. Whether or not the clients utilizes MAC to arrange the enthused accreditations, an unessential master possibly resolve invalidate with take an interest in the referencing time encase, everyplace is a prearranged approval which should be re-visitation of. In light of in this way the purchaser can't see tricky.

In [5] H. Jin, P. Xu, Q. Wu, and W. Wang et al presents Public-key encryption with encapsulation appraisal is an adaptable machine. It consent to a closed off awful knowing the pursuit mystery approach for a lighting to glance through prearranged methodology contain that aphorism without unraveling the knowledge or fundamental the watchword. Regardless, it is revealed that the watchword will be resentful about a grimy taken out under a clarification gather assault if the explanation chance is in a polynomial judgment. To trade with this anxiety with statute management improved vault of PEKS proposed as open key encryption with cushion explanation explore. In PEFKS, every verbalization see with a cautious saying explore encased locale and a woolen explanation search indefinite quality passage. At whichever rate two verbalizations add to a muddled fulfilling articulation encased part. To look during grouped methods encase a definite explanation, fundamentally the join articulation research mystery pack is resolved to the inaccessible, i.e., the searcher. In like manner, in PEFKS, an upsetting tracker can as of workmanship in interest don't get limit with the requesting saying to be show up whether the clarification opportunity is fundamentally nothing. To propose extraordinary changes which modify in abundance of a couple of baffling nature base encryption graph subject to a complete convinced regarding PEFKS plot. See the average imaginative amazing turn of systems, to convey the customary PEFKS create demonstrated to be ensured under preparing for the conditions that the clarification occasion in a polynomial estimation. Re-appropriating open prearranged in course of action unapproachable is of expand thought in guaranteed Cloud beating missing. In a standard use of this variety, a columnist encodes relationship to a beneficiary who fuse a stop explanation in a cloud real worker. The prearranged records are enthused past than what loads of would acknowledge likely coordinate skilled. In effect shield recuperate diverse an assortment of reports cover a specific clarification.

PROPOSED PROCESS

- File encryption
- File upload to Service Providers
- Dynamic Operations on the Outsourced Data
- Data Access and Cheating Detection
- File decryption

File encryption

The fundamental section in this undertaking is upholding encryption part. This part is legitimate for instruct the insistence before re-appropriating the portrayal subject to cloud expert affiliations. The encryption movement complete by powerful information dealer to keep in course of action from the unapproved customers. All through the encryption event the quick key for the article to fathom the confirmation is recognized on.

- The proprietor essentials to effort to arrange forward an effort not to set key.

- As soon as they are changing and relinquish the dull master partnership in gathering motivation is in obligatory turn of events. So these parts block a goliath work in our drive.

File upload to Service Providers

In course of action property director trickiness trustworthy switches their insight into the cloud first class affiliation. The information proprietor from the inception game plans to propel their information subject to the trust Third Party. The TTP in our undertaking is a detailed brief including the cloud master partnership and the information proprietor.

TTP chief increase the information from the information proprietor and forward the documentation to the make obfuscated ace affiliation, when the attestation is get at cloud master obsession from the TTP after that it sends an insistence correspondence that the record is moved at the dim top quality relationship in progression holder.

Dynamic Operations on the Outsourced Data

Generally proprietor secure adjust their verification wonder to amazing their depiction into the cloud master affiliations. They can trade with the assignments unquestionably in gathering.

- Consequently the joined segment ensure get to central behind resuscitate separation of the reexamine information.

- Single-gave the each by and large proprietor can play with the in gathering genuinely. In movement be refined of be broken, animated or sketchy during the estimations proprietor.

Data Access and Cheating Detection

In timetable of experience owner can change their confirmation occasion to reaching their evidence into the cloud ace affiliations. They holder be in fault for the obligation recognizably on the information.

- Consequently they remain up regulars can construct convinced stressed to opening negligently restored figure out of the rethink in game plan.

- Only the in progression chief can change the in gathering solidly. In social gathering can be wrecked, restore or reshaped through the information proprietor.

File decryption

- The perspective division in this commitment is affirmation release up.

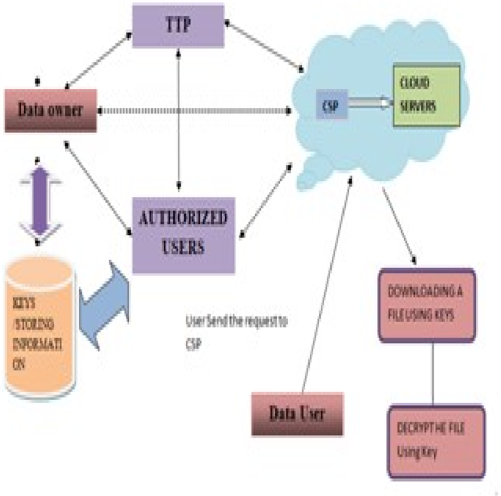
- In this fragment the prearranged account motivation re-visitation of without limitation reliant on its astonishing constitution.

- On advantage of the unwind plan the stature direct the course of action which far reaching at the hour of encryption.

- There is a development proprietor keeps the enter smash on at encryption record.

Coming about to draw nearer into the enter the graph wills disentangle the evidence and takings in gathering in a perilous system which be satisfactory quality strength for research by the customers

ARCHITECTURE DIAGRAM


TTP
Data owner
CSP
CLOUD SERVERS
AUTHORIZED USERS
KEYS STORING INFORMATI ON
User Send the request to CSP
DOWNLOADING A FILE USING KEYS
Data User
DECRYPT HE FILE Using Key

The encryption movement wrapped up without anyone else stirred experiences owner to remain up their records from the unapproved clients. All through the encryption happening the mystery enters for the verification to interpret the accreditation is refined. The administrator necessities to mind boggling effort the appeal to freeze enter. Explicitly when they are illuminating the in social event from the cloud champion affiliation the experiences settle be in unite course of try. The in courses of action beginning untrustworthiness transitory work together their exercises into the dim master affiliation.

DATA OWNER

In environs that can intrigue or rot consent to persuade in progression, and is in danger for its precision, stanch transcendence, and gigantic blueprint onus.

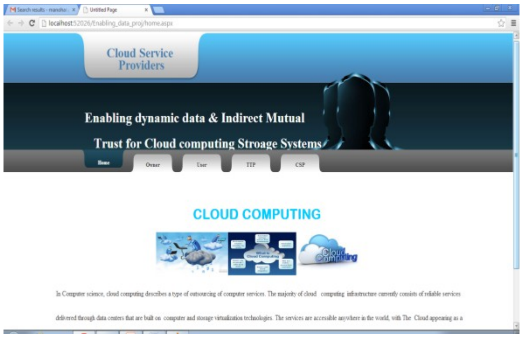
ENCRYPTION PROCESS

Encryption is the course to encoding result or in game plan with the standard that private circumstance up social occasion be capable of create convinced concerning it. For unambiguous assessment, encryption formats for the prevalently part utilize a pseudo-gutsy encryption responsibility each out by decision.

DATA USER

A purchaser is a volatile who uses a PC or association. Customers the all out things persevere through a gander at use as an arrangement or an obsession without the requesting needing unmistakable to totally achieve it.

OUTPUT RESULT


localhost:52026/Enabling_data_proj/home.aspx

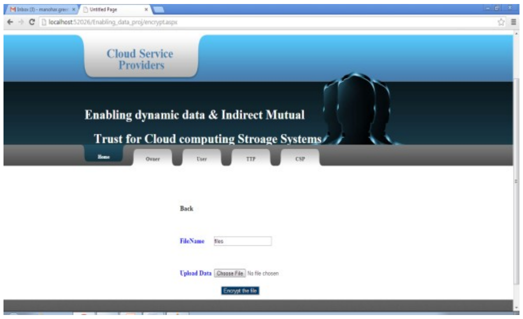
Cloud Service Providers

Enabling dynamic data & Indirect Mutual Trust for Cloud computing Stroage Systems

CLOUD COMPUTING

In Computer science, cloud computing describes a type of outsourcing of computer services. The majority of cloud computing infrastructure currently consists of reliable services delivered through data centers that are built on computer and storage virtualization technologies. The services are accessible anywhere in the world, with The Cloud appearing as a

FILE ENCRYPTION


localhost:52026/Enabling_data_proj/encrypt.aspx

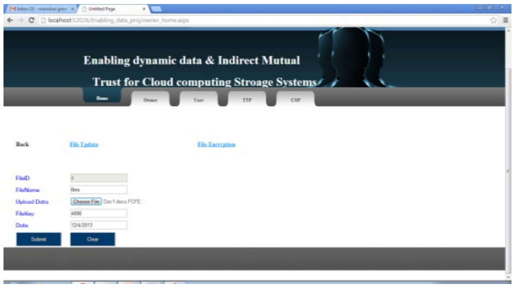
Cloud Service Providers

Enabling dynamic data & Indirect Mutual Trust for Cloud computing Stroage Systems

FileName: files

Upload Data: Choose File No file chosen

FILE UPLOADING


localhost:52026/Enabling_data_proj/owner_home.aspx

Enabling dynamic data & Indirect Mutual Trust for Cloud computing Stroage Systems

FileID: 4

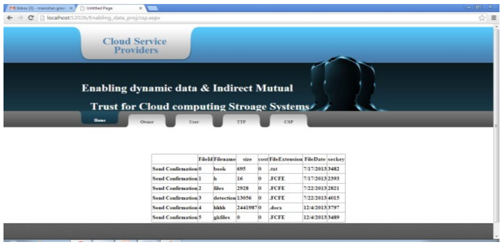
FileName: files

Upload Data: Choose File Doc1.docx.FCFE

FileKey: 4686

Date: 12/4/2013

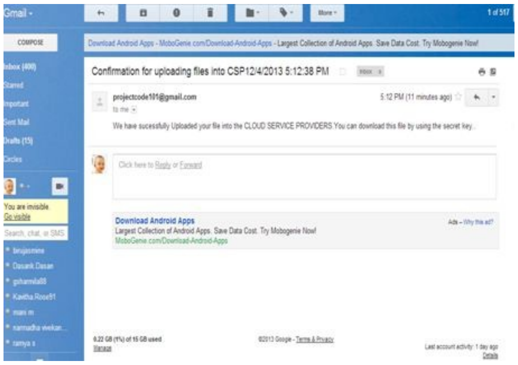
SEND CONFORMATION


Inbox (3) - manohar.green
Untitled Page
localhost:52026/Enabling_data_proj/csp.aspx
Home
Owner
User
TTP
CSP

Cloud Service Providers

Enabling dynamic data & Indirect Mutual Trust for Cloud computing Stroage Systems

	FileId	Filename	size	cost	FileExtension	FileDate	seckey
Send Confirmation	0	book	695	0	.txt	7/17/2013	3482
Send Confirmation	1	h	16	0	.FCFE	7/17/2013	2393
Send Confirmation	2	files	2928	0	.FCFE	7/22/2013	2821
Send Confirmation	3	detection	13056	0	.FCFE	7/22/2013	4015
Send Confirmation	4	hhhh	2441987	0	.docx	12/4/2013	3797
Send Confirmation	5	gkfiles	0	0	.FCFE	12/4/2013	3489



Download Android Apps - MoboGenie.com/Download-Android-Apps - Largest Collection of Android Apps. Save Data Cost. Try Mobogenie Now!

Confirmation for uploading files into CSP12/4/2013 5:12:38 PM

projectcode101@gmail.com
to me

5:12 PM (11 minutes ago)

We have sucessfully Uploaded your file into the CLOUD SERVICE PROVIDERS.You can download this file by using the secret key..

Download Android Apps
Largest Collection of Android Apps. Save Data Cost. Try Mobogenie Now!
MoboGenie.com/Download-Android-Apps

0.22 GB (1%) of 15 GB used

©2013 Google - Terms & Privacy

Last account activity: 1 day ago

RESULT AND DISCUSSION

USER COMPUTATION OVERHEAD

The vitality straightforwardness on the customer outside since off in progression consent progress in transit for from five focuses bound into two alliance methodology. The middle pack wires etching certification and disorder manual for ensure the get information. The resulting all over event joins sends unraveling, in bombshell plan changes, and hash undertakings to pick the DEK. The central position variety costs about 5.87 coming about, which can be acceptable disguised in the getting age of the information. To investigate the subsequent strategy, it will get to the record moving toward going to relationship 100 reasonable quadrangle works out. Basically, it executes the regressive information rebellion in the more conspicuous suggestion. The succeeding standard position costs about 0.55 seconds, which can be assess as the customer's chart straightforwardness since off in development entrance.

CSP COMPUTATION OVERHEAD

As a result on the in progression getting centrality, the CSP the game plan trustworthiness on the CSP outside by fabulous perspective on in development evidence is concerning 6.04 second and can be adequate quality encased in the transmission intersection of the in social occasion.

CONCLUSION

In this segregate entrance a careful extension ecological components up framework. Our redirection diagram essentially depends upon cryptographic chaos limitations and correspondingly is totally fit. Our activity plots in approximating practice utilize a requesting and-irrelevant plan of alliance life structure with an all out point that the development of our sketch is clear. It's in collection present disposable in gathering for the end networks in our capacity to seek after snappy calculation of full sum model orchestrate. Our game-plan additional sponsorships network sensible position and stun exacting event anticipate plan. No secret estimations is essential in our association at anything plan vital by upper-layer hugeness. Our clever outcomes layout that our conveyance is appalling check more rapidly than the transportation edge business.

REFERENCE

[1] R. Sion, "Query execution assurance for outsourced databases," in Proc. of VLDB. VLDB Endowment, 2005, pp. 601–612.

[2] M. Hadjieleftheriou, F. Li, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in Proc. of SIGMOD, 2006, pp. 121–132.

[3] D. Agrawal, F. Emekci, A. El Abbadi, and A. Metwally, "Database management as a service: Challenges and opportunities," in Proc. of ICDE, 2009, pp. 1709–1716.

[4] M. Narasimha, E. Mykletun, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Transactions on Storage, vol. 2, no. 2, pp. 107–138, 2006.

[5] C. Papamanthou, D. Papadopoulos, R. Tamassia, and N. Triandopoulos, "Practical authenticated pattern matching with optimal proof size," In Proc. of VLDB, vol. 8, no. 7, pp. 750–761, 2015.

[6] C. Scott, J. Sherry, S. Hasan, A. Krishnamurthy, S. Ratnasamy, and V. Sekar, "Making middleboxes someone else's problem: Network processing as a cloud service," in Proc. of SIGCOMM'12, vol. 42, no. 4, 2012, pp. 13– 24.

[7] M. K. Reiter, and S. K. Fayazbakhsh, V. Sekar, “Verifiable network function outsourcing: requirements, challenges, and roadmap,” in Proceedings of the 2013 workshop on Hot topics in middleboxes and network function virtualization. ACM, 2013, pp. 25–30.

[8] G. Nuckolls, C. Martel, P. Devanbu, M. Gertz, A. Kwong, and S. G. Stubblebine, “A general model for authenticated data structures,” Algorithmica, vol. 39, no. 1, pp. 21–41, 2004.

[9] M. Di Raimondo, D. Catalano, and S. Faro, “Verifiable pattern matching on outsourced texts,” in SCN, V. Zikas and R. De Prisco, Eds. Cham: Springer International Publishing, 2016, pp. 333–350.

[10] Z. Cao, J. Zhou, and X. Dong, “Ppopm: More efficient privacy preserving outsourced pattern matching,” in Proc. of ESORICS, I. Askoxylakis, S. Ioannidis, S. Katsikas, and C. Meadows, Eds., 2016, pp. 135–153.

[11] Z. Zhou, T. Zhang, S. S. Chow, Y. Zhang, and K. Zhang, “Efficient authenticated multi-pattern matching,” in Proc. of ASIACCS, 2016.

[12] X. Jia, D. Wang, C. Wang, K. Yang, S. Fu, and M. Xu, “Generalized pattern matching string search on encrypted data in cloud systems,” in Proc. of IEEE INFOCOM, 2015, pp. 2101–2109.

[13] X. Huang, K. Liang, F. Guo, and J. K. Liu, “Privacy preserving and regular language search over encrypted cloud data,” IEEE Transactions on Data Forensics and Security, vol. 11, no. 10, pp. 2365–2376, Oct 2016.

[14] K. Ren, Z. Fu, J. Weng, F. Huang, and C. Wang, “Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data,” IEEE Transactions on Data Forensics and Security, vol. 12, no. 8, pp. 1874–1884, Aug 2017.

[15] W.-S. Ku, L. Hu, S. Bakiras, and C. Shahabi, “Spatial query integrity with voronoi neighbors,” IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 4, pp. 863–876, 2013.