International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Geometric Range Queries on Encrypted Spatial Data using hybrid AES and Tiny algorithm

Jyoti[1], Neeraj Verma[2], Dr.Pratima Kumar[3]

[1]Student, Department of Computer Science Engineering, Prannath Parnami Institute of Management and Technology, Hissar, Haryana, India

[2]Assistant Professor, Department of Computer Science Engineering, Prannath Parnami Institute of Management and Technology, Hissar,Haryana, India

[3]Professor, Prannath Parnami Institute of Management and Technology, Hissar,Haryana, India

ABSTRACT

Accessible encryption is a procedure to perform significant questions on encoded information without uncovering protection. Be that as it may, geometric range look on spatial information has not been completely examined nor boosted by existing accessible encryption plans. In this we plan a symmetric-key accessible encryption conspire that can boost geometric range inquiries on encoded spatial information. One of our real commitments is that our outline is a general approach, which can boost diverse sorts of geometric range questions. At the end of the time, our outline on encrypted information is free from the states of geometric range queries. In addition, we additionally expand our plan with the extra utilization of hybrid AES-Tiny to accomplish look multifaceted nature that is speedier than linear.

Keywords : Geometric range search, spatial data and encrypted data.

I. INTRODUCTION

Recently, the network intrusion detection community has made large-scale efforts to collect network audit logs from different sites. In this application, a network gateway or an Internet Service Provider (ISP) can submit network traces to an audit log repository.

However, due to the presence of privacy sensitive information in the network traces, the gateway will allow only authorized parties to search their audit logs. We consider the following four types of entities: a gateway, an untrusted repository, an authority, and an auditor. We design a cryptographic primitive that allows the gateway to submit encrypted audit logs to the untrusted repository. Normally, no one is able to decrypt these audit logs. However, when malicious behavior is suspected, an auditor may ask the authority for a search capability. With this search capability, the auditor can decrypt entries satisfying certain properties, e.g., network flows whose destination address and port number fall within a certain range. However, the privacy of all other flows should still be preserved. Note that in practice, to avoid a central point of trust, we can have multiple parties to jointly act as the authority. Only when a sufficient number of the parities collaborate, can they generate a valid search capability. We name our encryption scheme Range Query over Encrypted Data (RQED). In RQED, we encrypt a message with a set of attributes. For example, in the network audit log application, the attributes are the fields of a network flow, e.g., source and destination addresses,

port numbers, time-stamp, protocol number, etc. Among these attributes, suppose that we would like to support queries on the time-stamp t, the source address a and the destination port number p. Our encryption scheme provides the following properties:

• **Range query on attributes:** An authority can issue a decryption key for all flows whose (t, a, p) falls within a certain range: t ∈ [t1, t2] and a ∈ [a1, a2] and p ∈ [p1, p2]. Notice that range query implies equality and greater-than (smaller-than) tests, e.g., t ≥ t1 and a = a1 and p ≤ p1. With this decryption key, all flows whose (t, a, p) tuple falls within the above range can be decrypted.

• **Security requirement:** Normally, no one can learn any information from the ciphertexts. Under special circumstances, however, an auditor may obtain a decryption key from an authority for some range t ∈ [t1, t2] and a ∈ [a1, a2] and p ∈ [p1, p2]. For any flow, if at least one attribute among t, a, p lies outside the specified range, the auditor fails to decrypt it. The auditor inevitably learns that the (t, a, p) tuple of this flow does not lie within the given range. However, apart from this information, the auditor cannot learn anything more about the flow. For example, the auditor cannot learn anything about attributes other than t, a, p; in addition, she cannot decide whether tt2, etc.

II. METHODS AND MATERIAL

1. Problem statement

We are among the earliest to study the problem of point encryption, range query, and conditional decryption of matching entries. We propose a provably secure encryption scheme that allows us to achieve these properties. It summarizes the asymptotic performance of our scheme in comparison with other approaches. We study the practical performance of RQED, and show that it makes the encrypted network range query application feasible. We also study the dual problem to RQED, where one encrypts under a hyper-range in multi-dimensional space, and decrypts under a point. We show that RQED implies a solution to its dual problem, which enables investors to trade stocks through a broker in a privacy-preserving manner.

2. Preliminaries

3. Threat Models

It is assumed that the communication between the client and the server is performed without any intermediary entity (for example, a fully trusted authority) and that the client is capable to properly protect the secret key used for the encryption. It is also assumed that the cloud server to be honest-but-curious, whose goal might be to obtain full access to the plaintext of the encrypted stored data without altering any data that is communicated between the client and the server. The paper does not address data integrity and availability threats which can be handled by other mechanisms.

4. Assumptions and Notations

The proposal is based on the AES-Tiny model. The two entities in the system are the legitimate client and the cloud server that interacts between each other as the model is executed. The architecture considers the participation of one client although more clients can participate as well. The client owns the d-dimensional data and outsources them to the server in an encrypted form, wishing to not be revealed to any unauthorized entity. The client also aims to be able to search the data while protecting their confidentiality. The client is assumed to be capable to properly protect the secret key for the data decryption process. Finally, the client's device is assumed to have some minimum power, for example for being able to process the encryption and decryption processes or to perform simple calculations in order to refine the queries' results if needed. The main burden of computation cost is

assigned to the cloud service, which is this assumed to have ample storage space and power resources to store and query encrypted data through its sharing database services for the client. All data are assumed to be protected using existing symmetric or asymmetric data encryption schemes, which are not the focus of this paper, though symmetric encryption is encouraged.

5. Previous Methods

Some SE schemes that help comparisons can perform rectangular range queries by applying various measurements. Be that as it may, those augmentations don't work with other geometric range regions, e.g., circles and polygons all in all. Wang at a proposed a plan, which especially recovers focuses inside a hover over encrypted information by utilizing an arrangement of concentric circles. Zhu et al. likewise fabricated a plan for roundabout range search over encrypted spatial information. Lamentably, these two plans only work for circles, and don't make a difference to other geometric zones. Ghinita and Rughinis outlined a plan, which underpins geometric range queries byutilizing Hidden Vector Encryption. Rather than encoding a point with a parallel vector of T2 bits, where T is the measurement estimate, it uses a various leveled encoding, which lessens the vector length to 2log2 T bits. Notwithstanding, its pursuit time is as yet direct with respect to the quantity of tuples in a dataset, which runs gradually finished vast scale datasets as well as debilitates proficient updates. Our current work shows a plan that can work discretionary geometric range queries. It use Bloom channels and their properties, where an information point is spoken to as a Bloom channel, a geometric range question is additionally shaped as a Bloom channel, and the aftereffect of an inward result of these two Bloom channels effectively shows whether a point is inside a geometric region. Its propelled form with R-trees can accomplish logarithmic hunt by and large. In spite of the fact that it additionally uses SSW as one of the building hinders, its tree-based list and exceptional plan with Bloom channels are totally not the same as then two-level file presented in this paper, where these critical contrasts keep this past plan from supporting productive updates and down to earth look time. Some different works think about secure geometric tasks between two gatherings (e.g., Alice and Bob), where Alice holds a mystery point and Bob keeps a private geometric range. With Secure Multi-party Computation (SMC), Alice and Bob can choose whether a point is inside a geometric range without uncovering privileged insights to each other. Be that as it may, the model of these examinations are not the same as our own (i.e., Alice and Bob both give singular private data sources, while a customer in our model has all the private information sources however the server has no private data sources). Additionally, SMC presents broad collaborations. Information usage strategy is performed over the plaintext look. Because of increment of the cloud users, look task is given significance. Normally, Boolean pursuit activity was performed over the server to yield better outcomes. This query neglects to give better security to the cloud information. At first, multi-watchword positioned look was presented by Information Retrieval System (IRS). Latent Semantic Analysis (LSA) was utilized to recover the coordinated information. Dormant esteems amongst terms and reports were utilized for finding the affiliation. Further, k-NN grouping strategy is utilized for creating the security record. Secure file was acquired from smaller than usual hash incorporate cryptography, picture handling and data recovery. The pattern contains hash works and modified visual words. It yields moderate execution in transformed visual words. The subject of cryptographic gives secure frameworks. The technique brings about higher stockpiling overhead and not ensures the security. A protection safeguarding model query task is done in two stages, specifically, Ranked over catchphrase search, look over organized information.

6. Proposed method

7. Proposed work for Tiny-Block hybridization in AES-128

One of the most common implementation of encrypting the data that is converting the plain text in to cipher text and decrypting the data is by using the single core system Here only one core is used irrespective of the size of the file which has to be encrypted or decrypted. This method will work slowly if the data file is big in size. It may work well for data files which are small but it is sure that it takes much longer time to encrypt and decrypt the data for bigger files. So as to overcome the above mentioned drawbacks and make improvements in the field of AES implementation, a parallel core processor is introduced in the paper. With this method we made improvements in the conventional methods by reducing the run time process. AES is a symmetric key segment cryptography procedure. AES block cipher has 128, 192 or 256 bit keys to encode and decode information in blocks of 128-bits. AES has a discrete key development stage for the increase of 128, 192 or 256-bit keys so that these keys can be helped in numerous circles of cryptography process [11].

A. For encryption, every round involves of the subsequent four steps:

A non-linear sub-byte replacement stage every byte is substituted with alternative allowing to a lookup counter (S-box). This stage is essentially a stand lookup exploiting a 16×16 matrix of byte standards termed as s-box. This matrix includes of each probable arrangements of an 8-bit order (2*8 = 16 × 16 = 256) [10][12]. It again, the s-box is not only a random variation of these capacities and there is an all-around measured method for formation the s-box tables [13]. Over the matrix that becomes functioned upon all over the encryption is identified as state. This alteration completed of 2 phases: (i). Multiplicative inverses of every byte in the state. (ii). the outcome in this step is gained from phase (i) by altering y = f(x) Change Rows – an inversion step where every row of the state is shifted regularly a positive number of times. Shift row convert the line of state which accumulative the offset of rotation moves left, first line unaffected. Another line loop left 1 byte, third line loop left 2 bytes, likewise 4th line loop 3 bytes [10][9]. The Inverse Shift Rows revolution achieves these circular shifts the further technique for every of the last three lines. Mix Columns – a mixing process which works on the columns of the state, merging the four bytes in every column. It creates complicate changes to columns in the state. Efficiently a matrix increase in GF (28) using prime poly m(x) =x8+x4+x3+x+1. Add Round Key – every byte of the state is joint with the round key; each round key is resulting from the cipher key using a key program. In this phase the 128 bits of state are bitwise XOR with the 128 bits of the round key. The process is perceived as a column wise procedure among the 4 bytes of a state column and single word of the round key. This conversion is as straightforward as would be sensible which supports in productivity though it also affects all of state. A small modification of this block based procedure can recover the entire text/data. Such modification of the block preparation of text is designated as S-Block retrieve. For instance, 4 × 4 non overlying blocks for storage in matrix formation shifted from standard and size **(N×M)** box which gotten through M rows from the top and *N* columns from left. Let us signify the cropped image by $\hat{I}_{u;v}$ **is (N-4) × (M-4).**

Let's denote the round based block

$$\grave{I}^{\sigma}_{u,v}\grave{I}^{\sigma}_{u,v} = I - \hat{I}_{u,v}$$

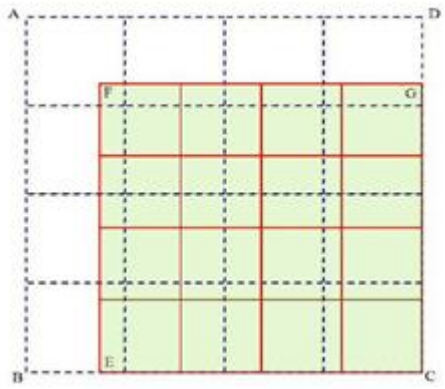

Figure 1 : Tiny S-Block based reconstruction from S-Box

Another possible way of retrieve is to use a block size other than 4 × 4 i.e. using blocks of sizes $m \times n$ where $m \neq 4$ and $n \neq 4$. In such a case, the quantization matrix Q has to be changed accordingly to size $m \times n$ at the time of data extraction.

The TEA is a kind of Feistel type ciphers which usages operations from mixed (orthogonal) arithmetical groups XOR, ADD and SHIFT. A dual shift causes all bits of the data and key to be assorted commonly.

The key program process is modest; the 128-bit key K is separated into four 32-bit blocks K = (K [0], K[1], K[2], K[3]). Tiny encryption algorithm aspects to be extremely resilient to difference cryptanalysis (Biham et al., 1992) and achieves whole dispersion (where a one bit alteration in the plaintext will cause about 32 bit differences in the cipher text). Time routine on a workstation is very stirring of this approach.

B. Steps involved in research

The Encoded file is in print on MATLAB platform and accepts a 32-bit word size. The 128 bit key is divided into four portions and is put in storage k [0] - k [3] and the Data is kept in v[0] and v[1].

1. Make m×n non-overlapping block separating size of AES-128 matrix
2. Let designate this set of blocks by $P_{I\,u,\,v}^{(m\times n)}$
3. Select a set of blocks from $P_{\hat{I}\,u,\,v}^{(m\times n)}$ (using a key common through both ends) and achieve the cypher text in every nominated blocks by every standard SHA based authentication scheme. The quantization matrix Q which is a shared secret is used for finding the quantized coefficients.
4. Apply DE quantization and Inverse for same size of block matrix would be extracted for small size of message.

The sender sends A to The receiver B.

Then Decryption side\

Receiver B essential does the subsequent:

1- Get the cipher text () from A.

2- Calculate (r) as follows:

$r = y^{p-1-x} \bmod p$

3- Improve the plaintext as follows:

$m = (r * z) \bmod p$

The TEA usages adding and calculation as the flexible operatives in its place of XOR. The TEA encryption routine depends on the alternative use of XOR and ADD to deliver nonlinearity. The procedure has 32 cycles (64 rounds). TEA is short sufficient to inscribe into virtually some sequencer on any computer.

The block based Tiny Encryption Algorithm (B-TEA) is a block cipher encryption procedure that is very modest to device has fast implementation time, and takings nominal storing space [2]

C. Authentication using SHA

SHA has a unique beneficiary hash purposes to SHA-1 & it is also one of the solidest hash purposes obtainable. Whereas SHA-1 has not been cooperated in real-world circumstances, SHA-256 is not much more composite to cipher. The 256-bit key creates it a decent partner utility for advance encryption

algorithm. It is definite in the NIST (National Institute of Standards and Technology) typical 'FIPS 180-4'. NIST similarly deliver a no. of test vectors to confirm accuracy of application.

1. FIPS 180-4 requires the communication has a '1' bit attached, and is formerly amplified to an entire quantity of 512-bit blocks, counting the text extent (in bits) in the last 64 bits of the previous block.
2. Subsequently user must have a byte-stream fairly than a bit-stream; calculation a byte '10000000' (0x80) adds the compulsory bit "1".
3. To change the text to 512-bit slabs, it compute the no of slabs essential, N, formerly for every these it will generate a 16-integer (i.e. 512-bit) collection. For every these numbers, It will take four bytes from the communication (using char Code At), and left-shift them through the suitable quantity to pack them into the 32-bit number.
4. The char Code At () technique proceeds NaN for out-of-bounds, then the '|' operative changes this to zero, so the 0-padding is completed indirectly on change into slabs.
5. Formerly the measurement of the message (in bits) wants to be added in the last 64 bits, that is the latter two numbers of the concluding block. In code, this could be done

```
M [N-1] [14] = ((msg.length-1)*8) >>> 32;
  M [N-1] [15] = ((msg.length-1)*8) &
0xffffffff;
```

On the other hand, JavaScript bit-ops change their influences to 32-bits, so n >>> 32 would provide 0. Therefore it uses mathematics operatives in its place: for the most-significant 32-bit quantity, it will distribute the (unique) extent through 2^32, and use floor () change the consequence to an integer.

Most important is that refunded is the recorded hexadecimal symbol of the second hash. This can be valuable for example for storage hashed PINs, but if it will want to usage the hash as a key to an encryption routine, for instance, you will famine to use the dual worth not this written illustration.

D. Encryption using Tiny-Block hybridization in AES-128

BLOCK –TINY

TEA is a modest but influential encryption procedure (grounded on a 'Feistel cipher'). TEA is a light-weight explanation more suitable for certain uses than 'manufacturing strength' methods such as AES which can be valuable for web uses that need safety or encryption. It will provide protected cryptology, robust encryption in a few outlines of brief. TEA form is nearer than the innovative (64-bit block form) when encoding longer slabs (ended 16 chars), and is new safe ('an individual bit will alteration around one partial of the minutes of the whole block, parting no place where the variations start'). It is also modest to implement for encoding arbitrary-length manuscripts (presence mutable block size, it needs no 'mode of operation'). The tiny encryption algorithm usages a 128-bit key which is used for increased safety and an encoded or hashed form of the complete password.

BLOCK-TINY and AES-128 operation

- Tiny encryption algorithm works as a Feistel system (a symmetric slab code) that usages a mixture of bit unstable, XOR, and enhance processes to generate the essential dispersal and misperception of data.
- It fixes these processes on 32 bit arguments slightly than single bytes, an identical significant optimization that the authors avoid "progressive the authority of a processor." It customs a 128 bit (4 word) key, involvement in its separate word

mechanisms in an actual key agenda.

- The innovative operation works on 64 bits (two words) of facts at a time, though options (such as Block TEA) permit arbitrary-sized blocks.

AES-128

We confine to depiction of a characteristic round of advance encryption algorithm. Every round include of four sub-processes. The 1st round procedure is represented below:-

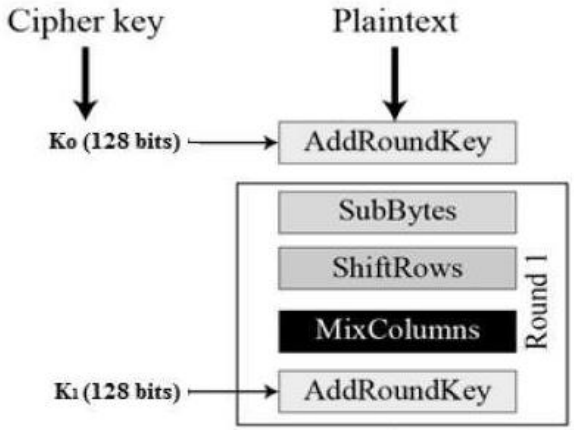

Fig. 2: Operation process of AES-128

Byte Substitution (Sub Bytes)

The 16 input bytes are replaced in observing up a secure table (S-box) assumed in strategy. The consequence is in a matrix of 4 rows and 4 columns.

Shift rows

All of the 4 rows of the matrix are removed to the left-hand. Some accesses that 'fall off' are re-inserted on the correct crosswise of row. Shift is approved out as surveys –

- 1st row is not removed.
- 2nd row is removed 1 (byte) location to the left.
- 3rd row is removed 2 locations to the left.
- 4th row is removed 3 positions to the left.
- The consequence is a novel matrix containing of the similar 16 bytes but removed w.r.t each other.

Mix Columns

Every column of 4 bytes is currently altered using a singular exact purpose. This purpose taking as input the four bytes of one column and productions four entirely new bytes, which change the unique column. The consequence is alternative novel matrix containing of 16 novel bytes. It must be well-known that this stage is not achieved in the previous round.

Add round key

The 16 bytes of the matrix are currently measured as 128 bits and are XORed to the 128 bits of the round key. In case this is the most recent round formerly the productivity is the cipher text. Then, the subsequent 128 bits are construed as 16 bytes and we instigate additional comparable round.

III. Result and discussion

This work presents the hybrid cryptography of the Tiny Encryption and AES-128 Set of rules. In this investigation we reviewed the best collective approaches in the cryptography of a slab cipher system for Geospatial on cloud. The resultant of Public-Key Processes is symmetric, that is to approximately use to encode the text or given text by user is different from the key used to decrypt the message. The encryption key, identified as the Public key which used to encode a communication, but the message can only be deciphered through the information that has the decryption key, recognized as the private key.

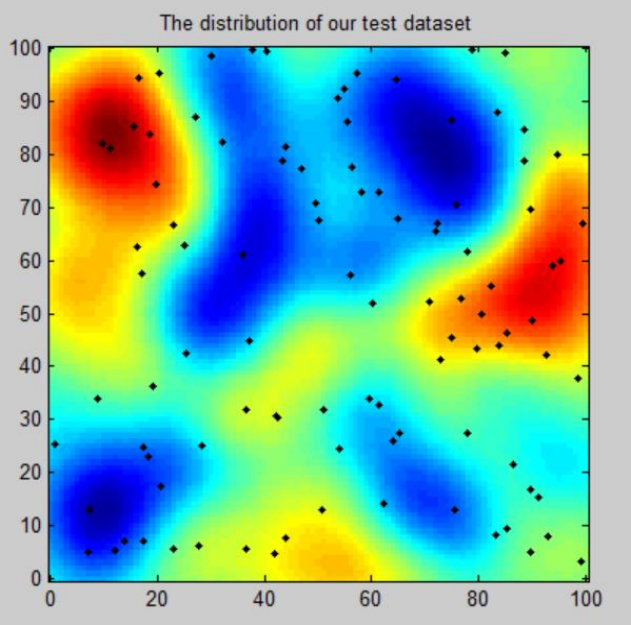

Figure 3: Distribution of Test Dataset such as high frequent clustered location in dark color and black data points are different location of dataset

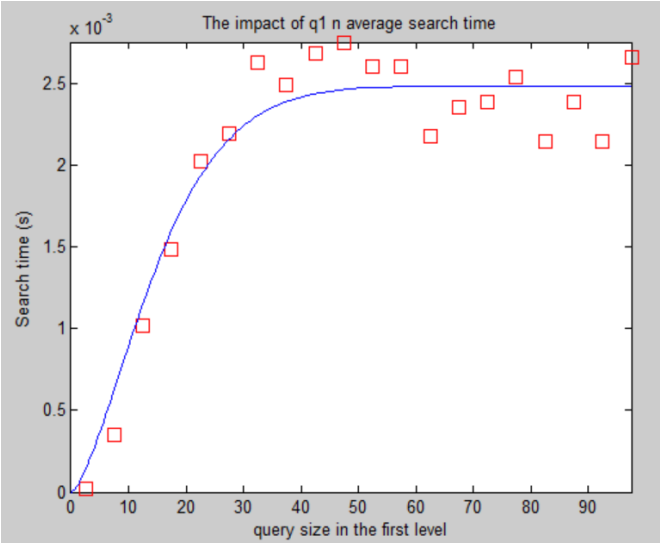

Figure 4: Searching time improvement for Distribution of Test Dataset with query size minimization in are different locations, red mark specification for base work fluctuation of time as far our proposed approach having sequential time

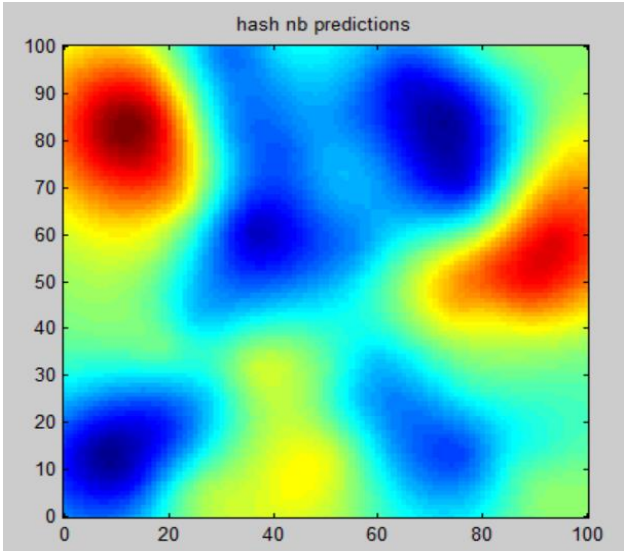

Figure 5: Different location , red mark specification for base work in low spots color and high contrast specification for our proposed approach having sequential data sizes using AES-TINY proposed

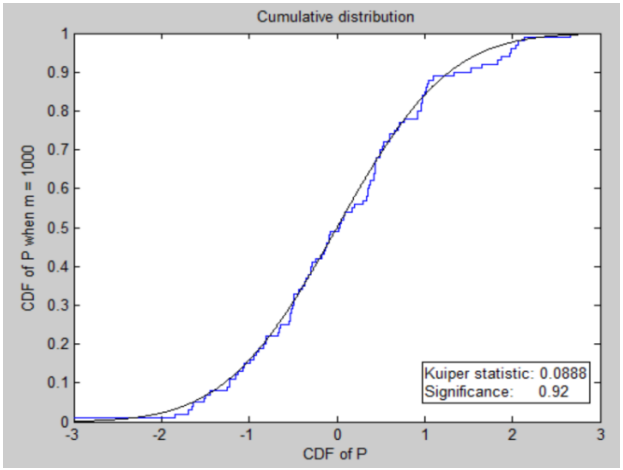

Figure 6: In blue line for different lat-long CDF for base work in line segment for our proposed approach having sequential data probability using AES-TINY proposed improving distribution capacity for various locations

IV. Conclusion

We study a hybrid AES-Tiny approach to securely search encrypted spatial data with geometric range queries. Specifically, our solution is independent with the shape of a geometric range query with the additional use of secure hash, our scheme is able to achieve faster-than-linear search complexity regarding to the number of points in a dataset. The

security of our scheme is formally defined and analyzed with in distinguishability under Selective Chosen-Plaintext Attacks. Our design has great potential to be used and implemented in wide applications, such as Location-Based Services and spatial databases, where the use of sensitive spatial data with a requirement of strong privacy guarantee is needed.

V. REFERENCES

1. R A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for orderpreserving encoding," in Proc. IEEE SP, May 2013, pp. 463-477.
2. F Kerschbaum and A. Schropfer, "Optimal average-complexity ideal- security order-preserving encryption," in Proc. ACM CCS, 2014, pp. 275-286.
3. B Wang, Y. Hou, M. Li, H. Wang, H. Li, and F. Li, "Tree-based multi-dimensional range search on encrypted data with enhanced privacy," inProc. SECURECOMM, 2014, pp. 1-25.
4. E-O. Blass, T. Mayberry, and G. Noubir, "Practical forward-secure range and sort queries with update-oblivious linked lists," in Proc. PETS, 2015, pp. 81-98.
5. B Wang, M. Li, H. Wang, and H. Li, "Circular range search on encrypted spatial data," in Proc. IEEE ICDCS, Jun./Jul. 2015, pp. 794-795.
6. Online]. Available: http://aws.amazon.com/solutions/casestudies/
7. D X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE SP, May 2000, pp. 44-55.
8. C Shahabi, L. Fan, L. Nocera, L. Xiong, and M. Li, "Privacy-preserving inference of social relationships from location data: A vision paper," in Proc. ACM SIGSPATIAL GIS, 2015, pp. 1-4.
9. B Chazelle, "Filtering search: A new approach to query-answering," SIAM J. Comput., vol. 15, no. 3, pp. 703-724, 1986.
10. P. K. Agarwal and J. Erickson, "Geometric range searching and its relatives," Discrete Comput. Geometry, vol. 223, pp. 1-56, 1999.
11. A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh,"Location privacy via private proximity testing," in Proc. NDSS, 2011.
12. H. Shirani-Mehr, F. Banaei-Kashani, and C. Shahabi, "Efficient reachability query evaluation in large spatiotemporal contact datasets," Proc.VLDB Endowment, vol. 5, no. 9, pp. 848-859, 2012.
13. M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars, Computational Geometry: Algorithms and Applications. Berlin, Germany:Springer-Verlag, 2008.
14. D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. Theory Cryptogr. (TCC), 2007, pp. 535-554