Secure Access of Encrypted Data Using Geographical Location

Mayur Gaikwad, Dinesh Gujar, Omkar Shelar, Prof. Vishal Valunj
D.Y.Patil School Of Engineering Academy,Ambi, Pune

ABSTRACT: Internet of Things (IoT) is associate additional and additional normal technological trend. The operation of IoT wishe s a sturdy data- handling capability, where most of {data|of information} is device data. Limitations associated with live, delaysin data amendment, and/or the requirement to preserve the privacy {of data|of data|of information} could result among the device knowledge doubted. Thus, one key challenge is "How can we tend to confirm the privacy of knowledge collected from IoT devices, considerably unsure data, that square measure being outsourced to the cloud for analysis, storage and archival?". Searchable encryption (SE) theme may be a promising technique that allows the wanting over encrypted (uncertain) data hold on offshore. throughout this Project Geo-distributed clouds offer associate intriguing platform to deploy on-line social network (OSN) services. To leverage the potential of clouds, a major concern of OSN suppliers is optimizing the money value spent in exploitation cloud resources whereas considering totally different important desires, additionally as providing satisfactory quality of service (QoS) and data accessibility to OSN users. throughout this paper, we tend to tend to review the matter of value improvement for the dynamic OSN on multiple geo-distributed clouds over consecutive time periods whereas meeting predefined QoS and data accessibility desires. we tend to tend to model the worth, the QoS, still as a result of the data accessibility of the OSN, formulate the matter, and elegance associate rule named cosplay. 10dency to|we tend to} offer enter depth experiments with a large-scale real-world Twitter trace over ten geo-distributed clouds all across the United States. Our results show that, whereas forever making sure the QoS and conjointly the data accessibility cosplay, can deflate much more one-time value than the progressive ways that, and it should conjointly significantly deflate the accumulative value once unceasingly evaluated over forty eight months, with OSN dynamics love real-world cases.

Index Terms: Online social network ,Cloud computing, optimization models and methods, performance analysis and evaluation

I INTRODUCTION

INTERNET of Things (IoT) devices, like sensing devices (e.g. Radio-Frequency Identication RFID, infrared device, world positioning system GPS, and device scanners), could also be accustomed facilitate intelligent identification, positioning, tracking, observation and management. Such information (also cited as device data) could also be random and incomplete in nature, partly due to limitations of deployed expelling instruments or delays in information amendment. In various words, the sensing element knowledge could also be inaccurate and unsure. the ability to manage unsure knowledge with efficiency is crucial in those in operation with information bases, etc. Thus, a way to with efficiency methodology unsure information can be a subject of ongoing interest to researchers. vary search can be a basic question performed on unsure information, whose purpose is to retrieve information within the question vary.

One example application of vary search in IoT is in agriculture Existing analysis on vary searches over multidimensional unsure information with Associate in Nursing arbitrary mainly follow the filtering and verification paradigm. By investment an efficient index structure, some objects could also be filtered at a threshold price whereas not conniving their look potentialities well. Also, existing analysis generally specialise in plaintext and can not ponder information interaction and sharing. a awfully vital medium for sensing element information interaction and sharing among the IoT is that the cloud, due to edges that might be completed like worth potency, high-capacity and therefore the reduction of overhead. as Associate in Nursing example, information

homeowners can most likely profit.

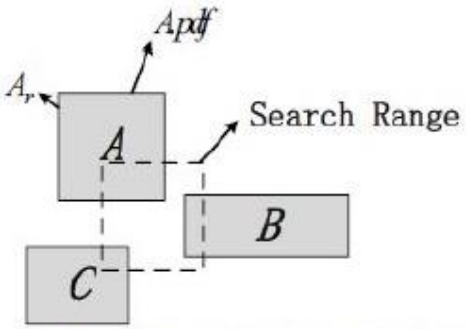


Fig. 1 Range search over sensor data

II LITERATURE SURVEY

1 An Ideal-Security Protocol for Order-Preserving Encoding
AUTHOR : Raluca Ada Popa, Frank H. Li
DESCRIPTION: Order-preserving encryption—an encryption scheme where the sort order of ciphertexts matches the sort order of the corresponding plaintexts—allows databases and other applications to process queries involving order over encrypted data efficiently. The ideal security guarantee for order-preserving encryption put forth in the literature is for the ciphertexts to reveal no information about the plaintexts besides order. Even though more than a dozen schemes were proposed, all these schemes leak more information than order. First order-preserving scheme that achieves ideal security. the main technique is mutable ciphertexts, meaning that over time, the ciphertexts for a small number of plaintext values change, and we prove that mutable ciphertexts are needed for ideal security. resulting protocol is interactive, with a small number of interactions. Here implemented our scheme and evaluated it on micro benchmarks and in the context of an encrypted MySQL database application. Here show that in addition to providing ideal security, our scheme achieves 1–2 orders of magnitude higher performance than the state-of-the-art order-preserving encryption scheme, which is less secure than our scheme

2. Order-Preserving Symmetric Encryption
AUTHOR : Alexandra Boldyreva, Nathan Chenette
DESCRIPTION: Initiate the cryptographic study of order-preserving symmetric encryption (OPE), a primitive suggested in the database community by Agrawal et al. (SIGMOD ’04) for allowing efficient range queries on encrypted data. Interestingly, we first show that a straightforward relaxation of standard security notions for encryption such as indistinguishability against chosen-plaintext attack (IND-CPA) is unachievable by a practical OPE scheme. Instead, we propose a security notion in the spirit of pseudorandom functions (PRFs) and related primitives asking that an OPE scheme look “as-random-as-possible” subject to the order preserving constraint. Then design an efficient OPE scheme and prove its security under notion based on pseudo randomness of an underlying block cipher. This construction is based on a natural relation uncover between a random order-preserving function and the hyper geometric probability distribution. In particular, it makes black-box use of an efficient sampling algorithm for the latter.

3. Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data
AUTHOR: Dario Catalano and Dario Fiore
DESCRIPTION: Here show a technique to transform a linearly-homomorphic encryption into a homomorphic encryption scheme capable of evaluating degree-2 computations on ciphertexts. Our transformation is surprisingly simple and requires only one very mild property on the underlying linearly-homomorphic scheme: the message space must be a public ring in which it is possible to sample elements uniformly at random. This essentially allows us to instantiate our transformation with virtually all existing number theoretic linearly-homomorphic schemes, such as Goldwasser- Micali, Paillier, or ElGamal. Resulting schemes achieve circuit privacy and are compact when considering a subclass of degree-2 polynomials in which the number of additions of degree-2 terms is bounded by a constant. As an additional contribution we extend our technique to build a protocol for outsourcing computation on encrypted data using two (non-communicating) servers. Somewhat interestingly, in this case boost a linearly-homomorphic scheme to support the evaluation of any degree-2 polynomial while achieving full compactness.

4. Optimal Average-Complexity Ideal-Security Order-Preserving Encryption
AUTHOR : F. Kerschbaum and A. Schroepfer

DESCRIPTION: Order-preserving encryption enables performing many classes of queries – including range queries – on encrypted databases. Popa et al. recently presented an ideal-secure order-preserving encryption (or encoding) scheme, but their cost of insertions (encryption) is very high. In this paper present an also ideal-secure, but significantly more efficient order preserving encryption scheme. this scheme is inspired by Reed's referenced work on the average height of random binary search trees. Here show that our scheme improves the average communication complexity from O(n log n) to O(n) under uniform distribution. Our scheme also integrates efficiently with adjustable encryption as used in CryptDB. In experiments for database inserts we achieve a performance increase of up to 81% in LANs and 95% in WANs

5. Indexing Uncertain Data in General Metric Spaces

AUTHOR : Fabrizio Angiulli and Fabio Fassetti

DESCRIPTION: Here deal with the problem of efficiently answering range queries over uncertain objects in a general metric space. In this study, an uncertain object is an object that always exists but its actual value is uncertain and modeled by a multivariate probability density function. As a major contribution, this is the first work providing an effective technique for indexing uncertain objects coming from general metric spaces. The generalize the reverse triangle inequality to the probabilistic setting in order to exploit it as a discard condition. Then, introduce a novel pivot-based indexing technique, called UP–index, and show how it can be employed to speed up range query computation. Importantly, the candidate selection phase of technique is able to noticeably reduce the set of candidates with little time requirements. Finally, provide a criterion to measure the quality of a set of pivots and study the problem of selecting a good set of pivots according to the introduced criterion. Here report some intractability results and then design an approximate algorithm with statistical guarantees for selecting pivots. Experimental results validate the effectiveness of the proposed approach and reveal that the introduced technique may be even preferable to indexing techniques specifically designed for the Euclidean space.

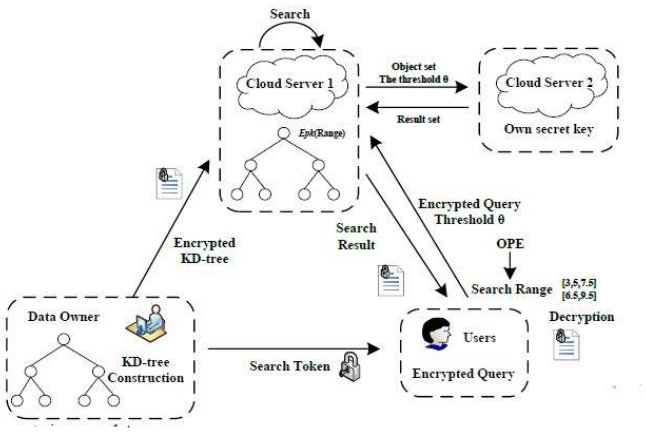
III PROPOSED SYSTEM:

By investing an efficient index structure, some objects may be filtered at a threshold worth while not conniving their look chances intimately. additional significantly, the models altogether such work don't capture the financial value of resource usage and therefore cannot work the cloud state of affairs.

IV ADVANTAGES:

INTERNET of Things (IoT) devices, such as sensing devices (e.g. Radio-Frequency Identification RFID, infrared sensor, global positioning system GPS, and laser scanners), can be used to facilitate intelligent identification, positioning, tracking, monitoring and management.

V SYSTEM ARCHITRECTURE:



VI MODULES:

- Data Owner: Which stores the data on cloud
- Data user: Data user which want the data from cloud.
- Cloud: Storing the data given by the Data owner and encrypt that data to store securely on cloud. Then this data is send to the user

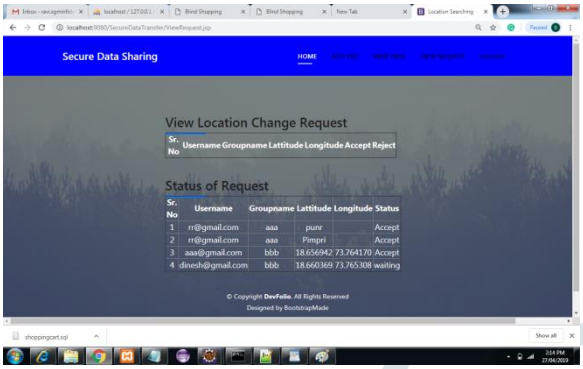
VII ALGORITHM DETAILS:

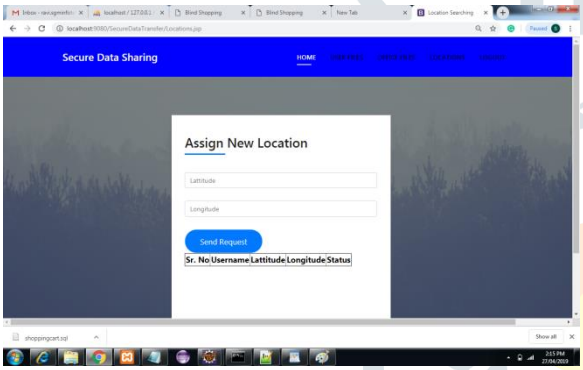
- KD Tree:
  - KD-tree can split the dataset evenly and support an efficient range search
- OPE:
  - To support comparison and additive operations, we apply homomorphic and

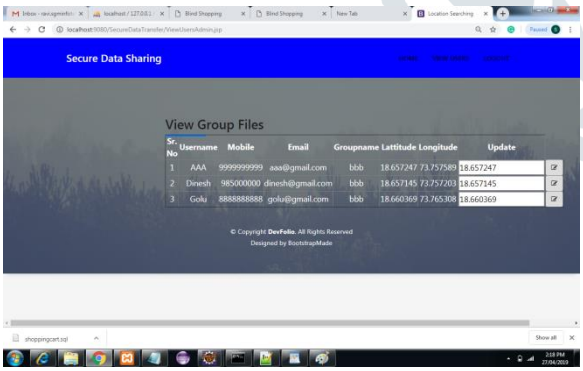
order-preserving encryption (OPE) encryption to encrypt the sensor data published by the data owners.

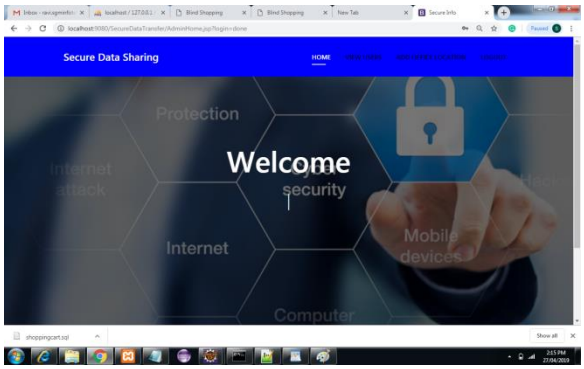
- HOMOMORPHIC ENCRYPTION:
  - OPE and homomorphic encryption simultaneously to encrypt the sensor data

VIII SCREEN SHOTS:









CONCLUSION:

The diversity and vary of IoT devices will grow as they are deployed throughout a broader vary of applications, ranging from civilian (e.g. wise cities and emergency response) to military and piece of ground (e.g. internet of Military Things and internet of piece of ground Things) then on. This reinforces the necessity to efficiently manage unsure and increasing amount of information from the IoT devices.

To ensure the security of unsure IoT data, notably those outsourced to the cloud or the sting, we've a bent to developed an honest assortment technique to support vary searches on multidimensional encrypted data. Specifically, among the planned theme, we've a bent to used the KD-tree to rearrange the objects to reinforce the retrieval efficiency. To support operations over ciphertext, we've a bent to used associate OPE and homomorphic writing theme to write down the dataset. we've a bent to then evaluated the security and performance of our theme.

REFRENCES:

[1] F. Angiulli and F. Fassetti, "Indexing Uncertain Data in General Metric Spaces," *IEEE Transactions on Knowledge & Data Engineering*, vol. 24, pp. 1640-1657, 2012.

[2] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on Theory and Application of Cryptographic Techniques*, 1999, pp. 223-238.

[3] R. A. Popa, F. H. Li, and N. Zeldovich, "An Ideal-Security Protocol for Order-Preserving Encoding," in *IEEE Symposium on Security and Privacy*, 2013, pp. 463-477.

[4] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-Preserving Symmetric Encryption," in *Advances in Cryptology - EUROCRYPT 2009, International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, 2009, pp. 224-241.

[5] B. Dan, E. J. Goh, and K. Nissim, *Evaluating 2-DNF Formulas on Ciphertexts*: Springer Berlin Heidelberg, 2005.

[6] D. Catalano and D. Fiore, "Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data," in *ACM Sigsac Conference on Computer and Communications Security*, 2015, pp. 1518-1529.

[7] F. Kerschbaum and A. Schroepfer, "Optimal Average-Complexity Ideal-Security Order-Preserving Encryption," pp. 275-286, 2015.

[8] J. Graff, *Introduction to Modern Cryptography*: Chapman & Hall/CRC, 2000.