ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Secure Encrypted Relational Data with using K-Nn Classification

**Bhaskar. S**
**M.E (CSE)**
**T.J. INSTITUTE OF TECHNOLOGY**
**Chennai, Tamilnadu.**

**D.Beulah Pretty**
**Associate Professor**
**T.J. INSTITUTE OF TECHNOLOGY**
**Chennai, Tamilnadu.**

**Abstract:**
***With the recent quality of cloud computing, users currently have the chance to source their information, in encrypted kind, still because the data processing tasks to the cloud. Since the info on the cloud is in encrypted kind, existing privacy-preserving classification techniques aren't applicable. During this paper, we tend to target resolution the classification drawback over encrypted information. Above all, we tend to propose a secure k-NN classifier over encrypted information within the cloud. The projected protocol protects the confidentiality of knowledge, privacy of user's input question and hides the info access patterns. The k-Nearest Neighbors formula could be a non-parametric methodology used for classification and regression. In each cases, the input consists of the k nearest coaching examples within the feature area. The output depends on whether or not k-NN is employed for classification or regression in k-NN classification, the output could be a category membership. Associate in nursing object is assessed by a majority vote of its neighbors. To the simplest of our information, our work is that the initial to develop a secure k-NN classifier over encrypted information beneath the semi-honest model. Also, we tend to through empirical observation analyze the potency of our projected protocol employing a real-world dataset beneath totally different parameter settings.***

**Keywords: Energy management, home automation, intelligent control system, wireless sensor network, ZigBee.**

## INTRODUCTION:

The cloud computing paradigm is revolutioni zing the organizations manner of operational their knowledge significantly within the manner they store, access and method knowledge. As Associate in Nursing rising computing paradigm, cloud computing attracts several organizations to contemplate seriously concerning cloud potential in terms of its value -efficiency, flexibility, and offload of body overhead. Most often, organizations delegate their procedure operations additionally to their knowledge to the cloud. Despite tremendous blessings that the cloud offers, privacy and security problems within the cloud area unit preventing corporations to utilize those blessings. Once knowledge area unit sensitive, the info got to be encrypted before outsourcing to the cloud. However, once knowledge area unit encrypted, no matter the underlying secret writing theme, playacting any data processing tasks becomes terribly difficult while not ever decrypting the info. There are a unit alternative privacy issues, incontestable by the subsequent example.Suppose Associate in nursing insurance firm outsourced its encrypted customer's information and relevant data processing tasks to a cloud. Once associate in nursing agent from the corporate desires to confirm the chance level of a possible new client, the agent will use a classification technique to work out the chance

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

level of the client. First, the agent must generate a knowledge} record letter of the alphabet for the client containing sure personal information of the client, credit score, age, legal status, etc. Then this record will be sent to the cloud, and therefore the cloud can work out the category label for knowledge record.All the same, since letter of the alphabet contains sensitive info, to safeguard the customer's privacy, letter of the alphabet ought to be encrypted before causing it to the cloud. The on top of example shows that {data mining data mothering} over encrypted knowledge (denoted by DMED) on a cloud additionally must defend a user's record once the record could be a a part of a knowledge mining process. Moreover, cloud can even derive helpful and sensitive info concerning the particular knowledge things by observant the info access patterns notwithstanding the info area unit encrypted

Therefore, the privacy/security necessities of the DMED downside on a cloud area unit threefold:

(1)Confidentiality of the encrypted knowledge,
(2)Confidentiality of a user's question record, and
(3)Activity knowledge access patterns.

Existing work on privacy protective data processing (PPDM) (either perturbation or secure multiparty computation (SMC) primarily based approach) cannot solve the DMED downside. Hot and bothered knowledge don't possess linguistics security, thus knowledge perturbation techniques cannot be wont to encode sensitive knowledge. Additionally the hot and bothered knowledge don't turn out terribly correct data processing results. Secure multiparty computation primarily based approach assumes knowledge area unit distributed and not encrypted at every collaborating party. Additionally, several intermediate computations area unit performed supported non-encrypted knowledge. As a result, during this paper, we tend to projected novel ways to effectively solve the DMED downside forward that the encrypted knowledge area unit outsourced to a cloud. Specifically, we tend to specialize in the classification downside since it's one amongst the foremost common data processing tasks.

## EXISTING SYSTEM:

Existing work on privacy-preserving data processing (PPDM) (either perturbation or secure multiparty computation (SMC) based mostly approach) cannot solve the DMED drawback. Rattled information don't possess linguistics security, thus information perturb bation techniques can't be accustomed code sensitive information. Conjointly the rattled information don't manufacture terribly correct data processing results. Secure multiparty computation based mostly approach assumes information area unit distributed and not encrypted at every taking part party. Additionally, several intermediate computations area unit performed supported non-encrypted information.

## DISADVANTAGE:

- In existing privacy-preserving classification techniques aren't applicable.
- In existing several intermediate computations area unit performed supported non-encrypted information.
- Data don't manufacture terribly correct data processing result
- Perturbed information don't possess linguistics security, thus information perturbation techniques can't be accustomed code sensitive information.

## PROPOSED SYSTEM:

We projected novel ways to effectively solve the DMED drawback presumptuous that the

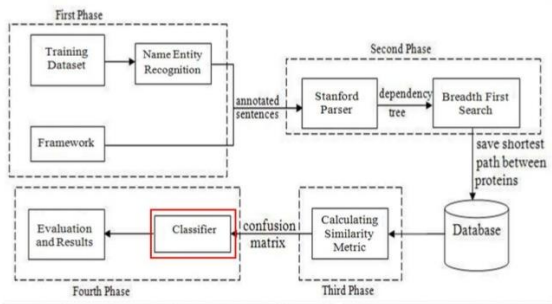
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

encrypted information are outsourced to a cloud. Specifically, we tend to concentrate on the classification drawback since it's one among the foremost common data processing tasks. As a result of every classification technique has their own advantage, to be concrete, this paper concentrates on capital punishment the k-nearest neighbor classification methodology over encrypted information within the cloud computing surroundings. During this paper, we tend to concentrate on resolution the classification drawback over encrypted information. Specifically, we tend to propose a secure k-NN classifier over encrypted information within the cloud. The projected protocol protects the confidentiality of information, privacy of user's input question, and hides the info access patterns. In our work is totally different from the key sharing primarily based resolution within the following facet. Solutions supported the key sharing schemes need a minimum of 3 parties whereas our work needs solely 2 parties. As an example, the constructions supported Share mind, a acknowledge SMC framework that relies on the key sharing theme, assumes that the amount of collaborating parties is 3.

## ADVANTAGES:

- In our projected we tend to are focusing the choice tree classifier and secure k-NN classifier.
- We concentrate on resolution the classification drawback over encrypted information.
- The projected protocol protects the confidentiality of information, privacy of user's input question, and hides the info access patterns.

## ARCHITECTURE DIAGRAM




## LITRETURE SURVEY:

### SECURE K-NEAREST NEIGHBOR QUERY OVER ENCRYPTED DATA IN OUTSOURCED ENVIRONMENTS

For the past decade, question process on relative information has been studied extensively, and plenty of theoretical and sensible solutions to question process are planned beneath numerous situations. With the recent quality of cloud computing, users currently have the chance to source their information also because the information management tasks to the cloud. However, as a result of the increase of varied privacy problems, sensitive information (e.g., medical records) got to be encrypted before outsourcing to the cloud. IN addition, question process tasks ought to be handled by the cloud; otherwise, there would be no purpose to source the info at the primary place. To method queries over encrypted information while not the cloud ever decrypting the info may be a terribly difficult task. During this paper, we have a tendency to specialize in resolution the k-nearest neighbor (k NN) query downside over encrypted info outsourced to a cloud: a user problems associate encrypted question record to the cloud, and therefore the cloud returns the k nearest records to the user. We have a tendency to initial gift a basic theme and demonstrate that such a naive resolution isn't secure. To produce higher

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

security, we have a tendency to propose a secure in protocol that protects the confidentiality of the info, user's input question, and information access patterns. Also, we have a tendency to by trial and error analyze the potency of our protocols through numerous experiments. These results indicate that our secure protocol is incredibly economical on the user finish, and this light-weight theme permits a user to use any mobile device to perform the kNN question

### Verifiable Privacy-Preserving Multi-Keyword Text Search In The Cloud Supporting Similarity-Based Ranking

The growing quality of cloud computing, large quantity of documents are outsourced to the cloud for reduced management price and simple access. Though encoding helps protective user knowledge confidentiality, it leaves the well-functioning nonetheless practically-efficient secure search functions over encrypted knowledge a difficult downside. During this paper, we tend to gift a verifiable privacy-preserving multi-keyword text search (MTS) theme with similarity-based ranking to handle this downside. To support multi-keyword search and search result ranking, we tend to propose to create the search index supported term frequency and therefore the vector house model with trigonometric function similarity live to attain higher search result accuracy.To improve the search potency, we tend to propose a tree-based index structure and varied reconciling strategies for multi-dimensional (MD) algorithmic rule so the sensible search potency is far higher than that of linear search. To any enhance the search privacy, we tend to propose 2 secure index schemes to fulfill the rigorous privacy necessities below robust threat models, i.e., best-known cipher text model and best-known background model. Additionally, we tend to devise a theme upon the projected index tree structure to modify legitimacy examine the came back search results. Finally, we tend to demonstrate the effectiveness and potency of the projected schemes through in depth experimental analysis.

### Secure Knn Computation On Encrypted Databases

Service suppliers like Google and Amazon are going in the SaaS (Software as a Service) business. They flip their immense infrastructure into a cloud-computing atmosphere and sharply recruit businesses to run applications on their platforms. To enforce security and privacy on such a service model, we want to shield the info running on the platform. Sadly, ancient encoding strategies that aim at providing \unbreakable" protection are usually not adequate as a result of they are doing not support the execution of applications like info queries on the encrypted knowledge.

In this paper we have a tendency to discuss the final drawback of secure computation on AN encrypted info that captures the execution and security needs. As a case study, we have a tendency to target the matter of k-nearest neighbor (kNN) computation on AN encrypted info. We have a tendency to develop a replacement uneven scalar-product-preserving encoding that preserves a special sort of real. We have a tendency to use apsis to construct 2 secure schemes that support kNN computation on encrypted data; every of those schemes is shown to resist sensible attacks of a special information level, at a special overhead value

### APPROACHES:

### UPLOAD DATASET

To transfer knowledge set to the button click "Upload" on the screen that runs in background of the screen. That knowledge set stores into the information, we'll offer extra security for uploaded knowledge.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## SECURITY

Security will be outlined because the method of mining for implicit, antecedently unknown, and doubtless helpful info from our databases by economical information discovery techniques. It's one among the concealment info from third party.

## K-NN CLASSIFIER

K nearest neighbors could be a one among the module in our project that stores all on the market knowledge and classifies new sets supported a similarity live (e.g., distance functions). A case is assessed by a majority vote of its neighbors, with the case being allotted to the category commonest among its K nearest neighbors measured by 2 beginning or finish purpose operate.

## ENCRYPTION

Encryption is that the best thanks to accomplish knowledge security. To browse associate encrypted file, you need to have access to a secret key or watchword that allows you to rewrite it. Unencrypted knowledge is named plain text; encrypted knowledge is named as cipher text. We are able to use constant technology for each encoding and cryptography.

## DECRYPTION

Decryption is that the method of changing encrypted knowledge into its original type, thus it will be human intelligible knowledge. Encoding and cryptography shouldn't be confused with coding and secret writing, during which knowledge is reborn from one type to a different however isn't deliberately altered thus on conceal its content.

## CONCLUSION:

Classification is a vital task in several data processing applications like detection of fraud by MasterCard corporations and prediction of growth cells level in blood. To safeguard user privacy, varied privacy-preserving classifica tion techniques are projected within the literature for the past decade. Yet, the present techniques aren't applicable in outsourced info surroundings wherever the information resides in encrypted kind on a third-party server. On this direction, this paper projected a unique privacy-preserving k-NN classification proto col over encrypted knowledge within the cloud. Our protocol protects the confidentiality of the information, user's input question and hides the information access patterns. We tend to additionally evaluate the performance of our protocol below completely different parameter settings. Since rising the potency of SMIN is a vital commencement for rising the performa nce of our PP kNN protocol, we tend to conceive to investigate different and a lot of economical solutions to the SMIN drawback in our future work. Also, during this paper, we tend to use the well-known k-NN classifier and developed a privacy-preserving protocol for it over encrypted knowledge. As a future work, we are going to investigate and extend our analysis to alternative classification algorithms

## REFERENCES:

[1] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," *NIST special publication*, vol. 800, p. 145, 2011.

[2] S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Managing and accessing data in the cloud: Privacy risks and approaches," in *CRiSIS*, pp. 1 –9, 2012.

[3] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: practical access pattern privacy and correctness on untrusted storage," in *ACM CCS*, pp. 139–148, 2008.

[4] P. Paillier, "Public key cryptosystems based on compositedegree residuosity classes," in *Eurocrypt*, pp. 223–238, 1999.

[5] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "k-nearest neighbor classification over

semantically secure encrypted relational data." eprint arXiv:1403.5001, 2014.

[6] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *ACM STOC*, pp. 169–178, 2009.

[7] C. Gentry and S. Halevi, "Implementing gentry's fullyhomomorphic encryption scheme," in *EUROCRYPT*, pp. 129– 148, Springer, 2011.

[8] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.

[9] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in *ESORICS*, pp. 192–206, Springer, 2008.

[10] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *ACM Sigmod Record*, vol. 29, pp. 439–450, ACM, 2000.

[11] Y. Lindell and B. Pinkas, "Privacy preserving data mining," in *Advances in Cryptology (CRYPTO)*, pp. 36–54, Springer, 2000.

[12] P. Zhang, Y. Tong, S. Tang, and D. Yang, "Privacy preserving naive bayes classification," *ADMA*, pp. 744–752, 2005.

[13] A. Evfimievski, R. Srikant, R. Agrawal, and J. Gehrke, "Privacy preserving mining of association rules," *Information Systems*, vol. 29, no. 4, pp. 343–364, 2004.

[14] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *IEEE ICDE*, pp. 217–228, 2005.

[15] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in *IEEE ICDE*, pp. 601–612, 2011.

[16] M. Kantarcioglu and C. Clifton, "Privately computing a distributed k-nn classifier," in *PKDD*, pp. 279–290, 2004.

[17] L. Xiong, S. Chitti, and L. Liu, "K nearest neighbor classification across multiple private databases," in *CIKM*, pp. 840–841, ACM, 2006.

[18] Y. Qi and M. J. Atallah, "Efficient privacy-preserving k-nearest neighbor search," in *IEEE ICDCS*, pp. 311–319, 2008.

[19] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *ACM SIGMOD*, pp. 563–574, 2004.

[20] H. Hacig¨um¨ us¸, B. Iyer, C. Li, and S. Malhotra, "Executing sql over encrypted data in the database-service-provider model," in *ACM SIGMOD*, pp. 216–227, 2002.

[21] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidimensional range queries over outsourced data," *The VLDB Journal*, vol. 21, no. 3, pp. 333–358, 2012.

[22] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in *ACM SIGMOD*, pp. 139–152, 2009.

[23] X. Xiao, F. Li, and B. Yao, "Secure nearest neighbor revisited," in *IEEE ICDE*, pp. 733–744, 2013.

[24] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure *k*- nearest neighbor query over encrypted data in outsourced environments," in *IEEE ICDE*, pp. 664–675, 2014.

[25] A. C. Yao, "Protocols for secure computations," in *SFCS*, pp. 160–164, IEEE Computer Society, 1982.

[26] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game - a completeness theorem for protocols with honest majority," in *STOC*, pp. 218–229, ACM, 1987.

[27] O. Goldreich, *The Foundations of Cryptography*, vol. 2, ch. General Cryptographic Protocols, pp. 599–746. Cambridge University mPress, 2004.

[28] O. Goldreich, *The Foundations of Cryptography*, vol. 2, ch. Encryption Schemes, pp. 373–470. Cambridge University Press, 2004.

[29] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

proof systems," *SIAM Journal of Computing*, vol. 18, pp. 186–208, February 1989.

[30] D. Chaum, C. Cr´epeau, and I. Damgard, "Multiparty unconditionally secure protocols," in *STOC*, pp. 11–19, ACM, 1988.

[31] J. Camenisch and M. Michels, "Proving in zero-knowledge that a number is the product of two safe primes," in *EURO-CRYPT*, pp. 107–122, Springer-Verlag, 1999.

[32] Y. Huang, J. Katz, and D. Evans, "Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution," in *IEEE Security and Privacy*, pp. 272–284, 2012.

[33] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure twoparty computation using garbled circuits," in *Proceedings of the 20th USENIX conference on Security (SEC '11)*, pp. 35–35, 2011.

[34] M. Bohanec and B. Zupan. The UCI KDD Archive, 1997. http: //archive.ics.uci.edu/ml/datasets/Car+Evaluation.