International Journal of Engineering & Technology, 7 (3.34) (2018) 259-261

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Classification and Privacy Preserving Search of Multimedia Data

[1]J.Jeejo Vetharaj, [2]S.Selvanayaki, [3]M.B.Suseela

[1]Assistant Professor, Annai Vailankanni College of Engineering, Kanyakumari
[2,3]Assistant Professor, Veltech Multitech Dr.RR & Dr.SR Engineering College
**Corresponding author E-mail: [1]jeejovetharaj@gmail.com , [2]selvanayaki@veltechmultitech.org, [3]suseela@veltechmultitech.org*

Abstract

Classification, which is commonly used task in data mining applications separates the data present in the database based on some category. For years and years, considering the rise of several privacy issues, solutions in the form of theoretical and practical have been proposed for the classification problem under various security models. However, for the late Notoriety about cloud computing, clients presently have the chance on outsource their data, clinched alongside encrypted form, and also those information mining assignments of the cloud.. The data on the cloud which is in encrypted form, therefore existing privacy preserving classification techniques are not applicable. In this paper, we focus on finding solution for the classification problem over the encrypted data .Users can store their data with encryption by the use of ordered relational data. So, the data is obtained correctly without decrypting.

Keywords: *Outsourced database, data access patterns, privacy preserving classification.*

1. Introduction

Information mining need totally requisitions clinched alongside numerous zones for example, banking, medicine, experimental exploration and also around legislature orgs. Arrangement may be a standout amongst those regularly utilized errands in information mining provisions. To as long as decade, because of those Ascent from claiming Different security issues, A large number hypothetical Furthermore useful solutions for the issue have been recommended with different security models. However, with those late Notoriety about cloud computing, users presently need the chance with outsourcing their data, clinched alongside encrypted form, and also the information mining assignments of the cloud. As the information stored in the cloud may be on cipher text form, existing systems of privacy-preserving arrangement strategies would not relevant. In this paper, we concentrate on comprehending those arrangement issue through encrypted information

2. Rsa Cryptosystem

RSA will be a standout amongst the principal useful public-key encryption systems Also is broadly utilized for transmission of secure information. The encryption fact that state funded and contrasts from the unscrambling way which is held mystery. Clinched alongside RSA, this asymmetry will be In light of the useful challenge for factoring the item of two expansive prime numbers, the calculating issue. A client from claiming RSA makes et cetera publishes

An government funded key In light of two extensive prime numbers, alongside a assistant worth. The prime numbers must a chance to be held mystery. Anybody could utilize the general population enter should scramble An message, Be that as with presently distributed methods, In people in general fact that extensive enough, best somebody with information of the prime numbers camwood feasibly unravel those message. Encrypted imparted keys are passed by RSA to almost similar magic cryptography which thus might perform heft encryption and decryption solutions at much faster rate in terms of speed. Those RSA calculation includes four basic steps: (i)Way generation (ii)Key distribution (iii) Encryption (iv)Unscrambling.

RSA includes a form of state funded way Also An private magic. People in general enter could be known by everybody and may be utilized for encrypting messages. Those proposition is that messages encrypted for people in general key camwood best make decrypted done a sensible amount about duration of the time utilizing those private kind of key. Using RSA considering its basic principle, it is observed that it is practical to find three integers e, *d* and *n* which are very large positive such that with modular exponentiation for all *m*:

$$(m^e)^d \equiv m \pmod{n}$$

It will be very difficult to find the value of *d* even if the values of m, n or e are known

The order of the two exponentiations can be changed for some operations and the relation can be written as:

$$(m^d)^e \equiv m \pmod{n}$$

The private key is never distributed .The public key can be represented as public key (n, e). To compute the cypher key

$$c \equiv m^e \pmod{n}$$

where the value of m lies between 0 and n and also gcd (*m*,*n*) = 1

The cypher text can be decrypted by

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

The general way to generate keys for the RSA algorithm are as follows:

Let a and b be two different prime numbers. These integers a and

b are chosen as a random integer in order to avoid security attack. In order to make factoring little difficult, the integers must be identical in magnitude but 'not necessarily identical in length. By making a primarily test the prime numbers could be found out.

1. *n* which is used as the modulus for the public and private keys is computed as: n=a b. The key length is the length, which is most often expressed in bits.
2. Compute the value of 'λ' = φ (*a*) φ (*b*) = (*a* − 1) (*b* − 1) = *n* − (*a* + *b* − 1)
   φ - Euler'stotient function
3. Choose another integer *e* whose value lies between 1 and 'λ' and calculate the value of gcd (*e*, λ) = 1.
4. Find the value of *d* which is the modular multiplicative inverse of *e* (modulo λ) as given below
   $d \equiv e^{-1} \pmod{\lambda}$

To clearly state the process: the answer for *d* is found given the equation $e \equiv 1 \pmod{\lambda}$. If the values of *e* are small, then it is less secure. *e* will act as the public key exponent. *d* is considered as the private key exponent.
The public key includes the modulus *n* along with the public exponent *e*. The private key includes the modulus *n* along with the private exponent *d*, which must be kept secret. a, *b*, and λ must also be kept secret because d is calculated using them.

3. Encrypt the Datasets

The interpretation of information into mystery code. Encryption is the best approach to accomplish information security. To peruse a scrambled document, you should approach mystery key or secret key that empowers you to decode it. The non-encoded information is called plain content, scrambled information is alluded to as figure content.. Datasets will be encrypted by RSA algorithm. RSA is a calculation utilized by current PCs to scramble and unscramble messages. It is an uneven cryptographic calculation. Asymmetric implies that there are two diverse keys. This is likewise called open key cryptography, since one of them can be given to everybody. The other key must be kept private. It depends on the way that finding the components of a whole number is hard which we call it as the factoring problem. A client of RSA makes and afterward distributes the result of two substantial prime numbers, alongside an assistant esteem, as their open key. The prime elements must be kept secret.

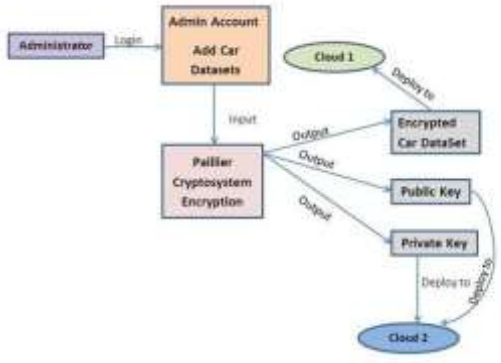
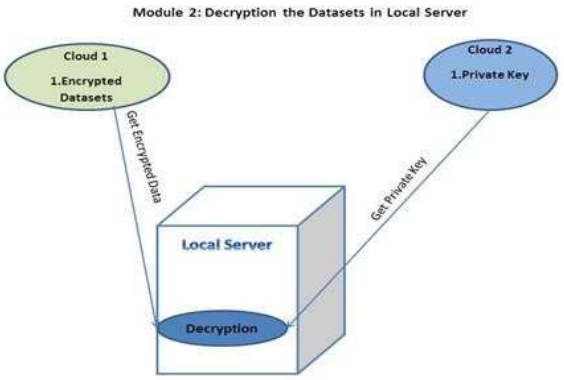


Fig 3.1: Encrypted Dataset

4. Decrypted Dataset

Deploying the encrypted Data in Cloud server and deploy the secret key in another Cloud Server. After Deploying the Datasets, Car company manager can give the queries related to the cars. For that we have to decrypt the car data sets using classifier. Suppose request from the manager hit the database, before hit the database we have to process the request using the method decrypt () method of RSA Cryptosystem algorithm and the method get_private_key(). Get_private_key is used to get the private key from the cloud server.



5. Classification of Data

After getting the decrypted car datasets and private key, we have to classify the car type. For that we are going to use Naïve Bayes classifier. In Naïve Bayes classification, the output is a class membership. Naive Bayes is a straightforward system for building classifiers, models that appoint class names to issue occurrences, spoke to as vectors of highlight esteems, where the class names are drawn from some limited set. It isn't a solitary calculation for preparing such classifiers, however a group of calculations in light of a typical rule. All Naïve Bayes classifier accept that the estimation of a specific esteem is autonomous of the estimations of some other element, given the class variable. For instance, an organic product might be red, round and around 10 cm in distance across.
A Naïve Bayes classifier considers each of these highlights to contribute autonomously to the likelihood that this natural product is an apple, paying little heed to any conceivable connections between's the shading, roundness and distance across highlights. For a few sorts of likelihood models, Naive Bayes classifiers can be prepared proficiently in an administered getting the hang of setting .In numerous useful applications, parameter estimation for Naive Bayes demonstrate utilizes the techniques for most extreme probability, as it were one can work with the Naive Bayes display without tolerating Bayesian Probability or utilizing any Bayesian strategies. Positives of Naive Bayes is that it just requires a little measure of preparing information to gauge the parameters important for characterization.

6. Conclusion

To secure client protection, different security safeguarding order methods have been proposed over the previous decade. The current methods are not pertinent to outsourced database conditions where the information dwells in encoded shape on an outsider server. We will propose a novel security safeguarding order convention over encoded information in the cloud. And also we will reduce the execution time of the encryption, decryption and classification.

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 Proc. 7th Int. Conf. Risk Security Internet Syst., 2012, pp. 1–9. 1272 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 5, MAY 2015

[3] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 139–148.
[4] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Techn., 1999, pp. 223–238.
[5] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "knearest neighbor classification over semantically secure encrypted relational data,"eprint arXiv:1403.5001, 2014.
[6] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Sympos. Theory Comput., 2009, pp. 169–178.
[7] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., 2011, pp. 129–148.
[8] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, pp. 612–613, 1979.
[9] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security: Comput. Security, 2008, pp. 192–206.
[10] R. Agrawal and R. Srikant, "Privacy-preserving data mining," ACM Sigmod Rec., vol. 29, pp. 439– 450, 2000.