ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Searching Data by Using Password Hashing Algorithm and Sorting Algorithm

Snehal Bansode[1], Prof. Prashant Jawalkar[2]

M.E. Student, Department of Computer, Bhivarabai Sawant Institute of Technology and Research, Wagholi, Pune, India[1]

Department of Computer, Bhivarabai Sawant Institute of Technology and Research, Wagholi, Pune, India[2]

ABSTRACT: In a full-text search, a search engine examines all of the words in every stored document as it tries to match search criteria (for example, text specified by a user). However, when the number of documents to search is potentially large, or the quantity of search queries to perform is substantial, the problem of full-text search is often divided into two tasks: indexing and searching. The indexing stage will scan the text of all the documents and build a list of search terms (often called an index,but more correctly named a concordance). In the search stage, when performing a specific query, only the index is referenced, rather than the text of the original documents. also using hashing password MD5 algorithm for secure password or authentication of specified user.

KEYWORDS: indexing, password hashing, Sorting.

I. INTRODUCTION

when the number of documents to search is potentially large, or the quantity of search queries to perform is substantial, the problem of full-text search is often divided into two tasks: indexing and searching. The indexer will make an entry in the index for each term or word found in a document, and possibly note its relative position within the document. Usually the indexer will ignore stop words (such as ”the” and ”and”) that are both common and insufficiently meaningful to be useful in searching. Some indexers also employ language specific stemming on the words being indexed. For example, the words ”drives”, ”drove”, and ”driven” will be recorded in the index under the single concept word ”drive” In this system focus on database passwords security, using a strong hashing algorithm and salting. Full-text search, unlike most of the topics in this machine learning series, is a problem that most web developers have encountered at some point in their daily work. A client asks you to put a search field somewhere, and you write some SQL along the lines of WHERE title LIKE :query. This provides a platform to eliminate the need to ever persist user password in plain text or easy to know any users password. This system is implemented using the message digest 5 (MD5) algorithms for hashing.

II. REVIEW OF LITERATURE

Fast Nearest Neighbor Search with Keywords[1] As per the paper Fast Nearest Neighbor Search with Keywords Yufei Taoand Cheng Sheng IEEE papar Conventional spatial queries, such as range search andnearest neighbor retrieval, involve only conditions on objects geometric properties. Today, many modern applications call for novel forms of queries that aim to find objects satisfying both a spatial predicate, and a predicate on their associated texts. For example, instead of considering all the restaurants, a nearest neighbor query would instead ask for the restaurant that is the closest among those whose menus contain steak, spaghetti, brandy all at the same time. Currently, the best solution to such queries is based on the IR2-tree, which, as shown in this paper. Securing Database passwords
using a combination of hashing and salting techniques[2] In this paper, focus on database password s security, using a strong hashing algorithm and salting. This provides a platform to eliminate the need to ever persist user password in

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

plain text or easy to know any users password. This system is implemented using the message digest 5 (MD5) algorithms for hashing

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

Our treatment of nearest neighbor search falls in the general topic of spatial keyword search, which has also given rise to several alternative problems.the searching is done with an effective secure and proper way. In every system authentication is very important and for good password authentication MD5 algorithem is used to give or provide secure password to the system. In this system the data can be indexes or inverted in proper tree format. Than which is useful to searching of data. Indexing is a data structure technique to efficiently retrieve records from the database files based on some attributes on which the indexing has been done. when the number of documents to search is potentially large, or the quantity of search queries to perform is substantial, the problem of fulltext search is often divided into two tasks: indexing and searching. The indexing stage will scan the text of all the documents and build a list of search terms. quick sort is used to sorting the records.

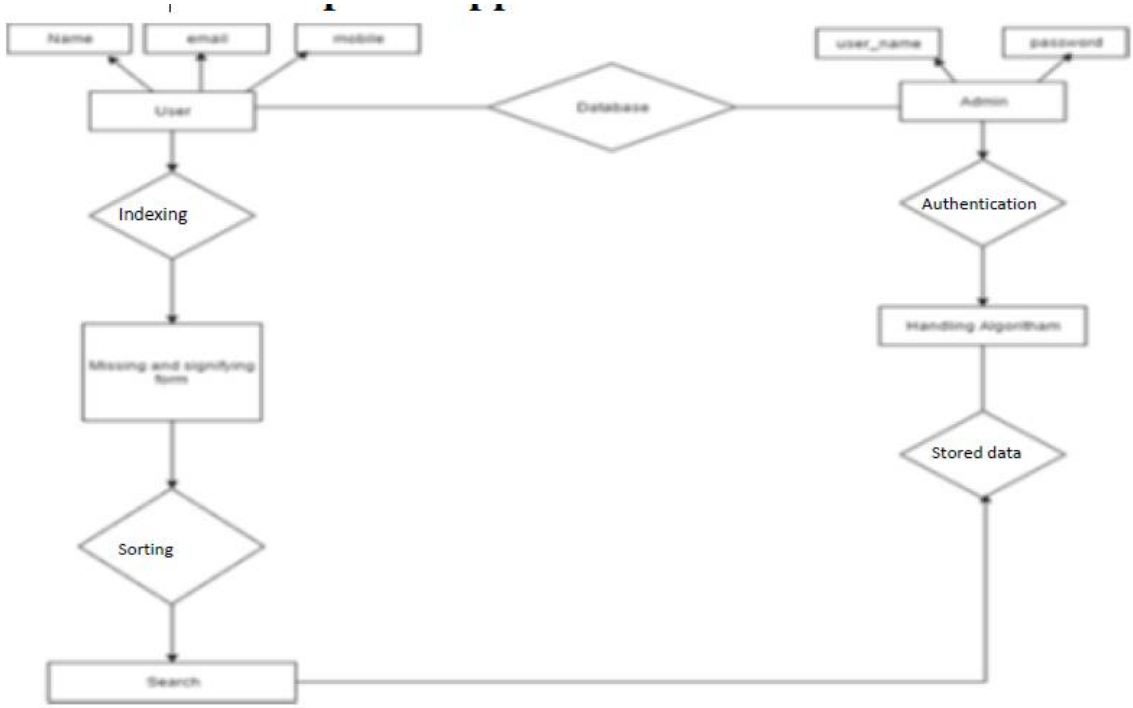

Fig. 1. System Arch.

The architecture diagram of the system shown below helps us to understand the system. The purpose of storing an index is to optimize speed and performance in finding relevant documents for a search query. Without an index, the search engine would scan every document in the corpus, which would require considerable time and computing power.user entered data into the system and also search data from the system by using full text search technique. And sort it according to quick sort and find the appropriate results.also used password hashing algorithem for Securing password.

1)Registered user- User registered there details and got password and user name and after login they fill the details of the missing and signifying people save that details in the database.

2)Administrator- admin is connected to data base. They retrieve records, change the records and handling it.also

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

admin search the record.also admin add the advertisement video and audio file.

IV. ALGORITHM PROPOSED

Algorithm 1 : MD5
MD5 algorithm can be used as a digital signature mechanism. This presentation will explore the technical aspects of the MD5 algorithm. It takes as input a message of arbitrary length and produces as output a 128 bit fingerprint or message digest of the input. It intended where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.

The main steps of MD5 algorithm to generate the hash value are given as below:
1) Append padding bits so message becomes 448 module 512.
2) Append length to the input message so that it becomes exact 64-bit in length.
3) Initialize the 32 bit MD buffer A, B, C, D.
4) Process the message in 16-word block,
F (X, Y, Z) = XY or not Z
G (X, Y, Z) = XZ or Y not
H (X, Y, Z) = X xor Y xor Z

I (X, Y, Z) = Y xor (X or not)

5) The final digest message will be stored in buffer.

Algorithm 2-Quicksort

Another divide and conquer algorithm:
Divide:
A[p...r] is partitioned (rearranged) into two nonempty subarrays A[p...q- 1] and
A[q+1...r] s.t. each element of A[p...q-1] is less than or equal to each element of
A[q+1...r]. Index q is computed here, called pivot.

Conquer: two subarrays are sorted by recursive calls to quicksort.

Combine:
unlike merge sort,no work needed since the subarrays are sorted in place already. The basic algorithm to sort an array A consists of the following four easy steps:
If the number of elements in A is 0 or 1, then
return
?Pick any element v in A. This is called the pivot
Partition A-{v} (the remaining elements in A) into two disjoint groups:
A1= {x?A-{v} | x=v}, and
A2= {x?A-{v} | x=v}
return
{quicksort(A1)followed by v followed byquicksort(A2)}
Small instance has
n=1
Small instance has
n=1
Every small instance is a sorted instance
To sort a large instance:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

select a pivot element from out of the n elements
Partition the n elements into 3 groups left, middle and right.
The middle group contains only the pivot element
All elements in the left group are = pivot
All elements in the right group are = pivot
Sort left and right groups recursively
Answer is sorted left group, followed by middle group followed
by sorted right group. Inverted indexes (I-index) have

[A] Benefits of proposed system- To find the Missing people or registered missing signifying peoples.This system is secure and password protected. Admin uplode adverisments and video ,audio on that site.

[B] Application- This system is used to find the missing peoples and accidental peoples information the other user easily saw the people information.

[C]Software Requirement Specification- Server Side:

Operating System :Windows XP/2007/2008
Platform : PHP
Front End :HTML,CSS
Editor : PHP development tool
Database : Mysql

V. CONCLUSION

Here this system proposed one system by using password hashing,MD5, and quick sort By using these we introduce one secure and useful system which is used to search the people who are missing and signifying and also used to post advertisement, audio, video.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my Guide (prof. P. B. Jawalkar) who gave me the golden opportunity to do this wonderful project on the topic DataMining , and security which also helped me in doing a lot of Research and I came to know about so many new things I am really thankful to them.Secondly I would also like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

REFERENCES

[1] B. Chazelle, J. Kilian, R. Rubinfeld, and A. Tal, “The Bloomier Filter: An Efficient Data Structure for Static Support Lookup Tables,” Proc. Ann. ACM-SIAM Symp. Discrete Algorithms (SODA), pp. 30- 39, 2004.
[2] Y.-Y. Chen, T. Suel, and A. Markowetz, “Efficient Query Processing in Geographic Web Search Engines,” Proc. ACM SIGMOD Intl Conf. Management of Data, pp. 277-288, 2006.
[3] E. Chu, A. Baid, X. Chai, A. Doan, and J. Naughton, “Combining Keyword Search and Forms for Ad Hoc Querying of Databases,” Proc. ACM SIGMOD Intl Conf. Management of Data, 2009.
[4] G. Cong, C.S. Jensen, and D. Wu, “Efficient Retrieval of the Top-k Most Relevant Spatial Web Objects,” PVLDB, vol. 2, no. 1, pp. 337- 348, 2009.
[5] C. Faloutsos and S. Christodoulakis, “Signature Files: An Access Method for Documents and Its Analytical Performance Evaluation,” ACM Trans. Information Systems, vol. 2, no. 4, pp. 267-288, 1984.
[6] Yufei Tao and Cheng Sheng, Fast Nearest Neighbor Search with Keywords”, 2014 IEEE
[7] Zhisheng L & Ken C. K. LEE, “IR-Tree: An Efficient Index for Geographic Document Search,” 2011.
[8] Nicholas Oluwole Ogini & Noah Oghenefego Ogwara, “Securing Database passwords using a combination of hashing and salting techniques,” 2014.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[9] G. Bhalotia, A. Hulgeri, C. Nakhe, S. Chakrabarti, and S. Sudarshan, "Keyword Searching and Browsing in Databases Using Banks," Proc. Intl Conf. Data Eng. (ICDE), pp. 431-440, 2002.
[10] X. Cao, L. Chen, G. Cong, C.S. Jensen, Q. Qu, A. Skovsgaard, D.Wu, and M.L. Yiu, "Spatial Keyword Querying," Proc. 31st Intl Conf. Conceptual Modeling (ER), pp. 16-29, 2012.
[11] X. Cao, G. Cong, and C.S. Jensen, "Retrieving Top-k Prestige- Based Relevant Spatial Web Objects," Proc. VLDB Endowment, vol. 3, no. 1, pp. 373-384, 2010.
[12] X. Cao, G. Cong, C.S. Jensen, and B.C. Ooi, "Collective Spatial Keyword Querying," Proc. ACM SIGMOD Intl Conf. Management of Data, pp. 373-384, 2011.