IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

Android Fuzzy Keyword Search In Encrypted Data Over Cloud

Pushpa Chutel,
Computer Science and Engineering RTMNU,
JIT, Nagpur.

Pallavi Chaowhan
Computer Science and Engineering RTMNU ,
JIT, Nagpur.

Pranjali Patil,
Computer Science and Engineering RTMNU
JIT, Nagpur.

Neha Khobragade
Computer Science and Engineering RTMNU
JIT, Nagpur.

Ankit Dangre
(Computer Science and Engineering RTMNU,
JIT, Nagpur

ABSTRACT:

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. We are developing this project for income tax, where we will store the tax details paid by the employees or businessman on android tablet. This data will be encrypted using 3DES Algorithm, Encrypted data will be stored in file and that file will be uploaded on Google Cloud. Finally, entire income tax data will be stored in encrypted mode onto cloud which will increase confidentiality and privacy of data.

KEYWORDS: Cryptography, Fuzzy Concept, Data Security

1. INTRODUCTION

Cloud is a space where the data is uploading and share data among multiple devices. This project is developing for income tax department, where peoples return income tax by using are android apk and income tax officer's stored official data on android tablet. This data will be encrypted using 3DES Algorithm, Encrypted data will be stored in file and that file will be uploaded on Google Cloud. Uploading confidential data files in encrypted mode on cloud through android tablet, so as to provide data security. The searching page is used to search the data. The keyword will be compared with confidential data on cloud which is encrypted files. Use fuzzy concept so as to correct misspelled word and search accurately. Appropriate searched data will be decrypted and shown to authenticated user.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that block adversaries various aspects in information security such as data confidentiality, data integrity, and authentication are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science and electronics and telecommunications. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same. Since World War 1 and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

As noted by the Institute for Security and Open Methodologies (ISECOM) in the OSSTMM, security provides "a form of protection where a separation is created between the assets and the threat." These separations are generically called "controls," and sometimes include changes to the asset or the threat.

2. LITRATURE SURVEY

In paper [1] gives cloud computing is mostly used to store the data. Cloud is way to centralize the all types of information. For providing security to all types of information and to store the confidential information more securely encryption is used. The information stored on cloud is encrypted. In the given paper it implements a technique to resolve the problems regarding to search data in cloud. In this paper the technique is applied for searching is that it encrypts the searchable keyword. Generally in keyword searching the user can make

ISSN 2348 – 7968

typographical mistakes so to avoid it the fuzzy concept is use. Fuzzy concept helps to autocorrect spellings. [1]

In paper [2] the searching technique is Improved and presented one method which uses different strategies on client as well as sever side to increase the efficiency of searching. To achieve the synonym construction of the keyword which is to be searched, the client can use English as well as Chinese, the establishment of the fuzzy-syllable words and synonym set of keywords and the implementation of fuzzy search strategy over the encryption of cloud data based on keywords. At client side the user enter their query keyword for search and at server side the select the data according to keyword and show in user understandable form. Fuzzy concept is useful for efficient use of historical results on basis of protection, security and privacy of data it helps to increase efficiency and take less time. [2]

The paper [3] gives, For efficient and effective use of searching encrypted data in cloud enable the keyword search directly to the data stored on cloud .In present solutions it provide multiple keyword exact search bus without any typographical error ,and in single keyword search it handle some typographical mistakes to certain extent. Fuzzy concept is used to correct the misspelled words. In this paper it implements a fuzzy search by putting some novel multi-keyword fuzzy search scheme for deriving benefits from the locality-sensitive hashing technique. Fuzzy matching is done by applying the algorithm rather than extending the file. It avoid to creating various indexes of keyword because it uses the historical search results. [3]

The paper [4] describes that, in modern cloud storage commodity the fuzzy search is very important to retrieve the information, suppose some cloud user pass their queries with some typographical errors or not having specified knowledge about the underlying keywords of stored data on cloud. In terms of privacy the data is encrypted before outsourcing to the cloud, which may be causes some dispute or misunderstanding regarding the data, data utilization flexibility and efficiency. In this paper it proposes, F2SE can achieve a top-k ranked fuzzy keyword search accordingly to the keyword similarity. In intervening of time it returns the keyword containing special hub strings customized by cloud user with deficient background knowledge, which can be used for undetermined search. [4]

3. PROPOSED WORK

The cloud commuting is mostly used for storing the data. To providing security to the data, need to protect data before uploading on cloud, for that encryption technique is applied on data. Data are encrypted before outsourcing. Most of the traditional searchable encryption scheme allows a user to perform searching over encrypted data securely. So that, it avoid the minor inconsistencies and minor errors in searching which done by user, the typical user behavior of searching and it happens frequently. This drawback makes the present techniques unsuitable in cloud computing and it greatly affecting the usability of the system, and making the user searching experience very frustrating and system efficacy very low.

The purpose of this paper is to provide the high degree of security to the device so that the attacker never gets the data in any way. The method we are applying is to securely providing encryption on one device but we can only decrypt it on another device. We are using for this the advantages of both type of encryption techniques i.e. Symmetric and Asymmetric encryption. We are encrypting the whole information or data using symmetric encryption technique. And the keys which are used to encrypt the data are securely encrypted by asymmetric encryption technique. As we are using both type of encryption we called it hybrid encryption. Main Objective of our project is cloud data security. Even though data files are stored in encrypted mode, searching is done with same accuracy in data files. Our objective is also to autocorrect misspelled words using fuzzy search concept. Searched Encrypted data is decrypted and shown in user friendly format.

Our project increases data security.
Our Project provides authentication.

3.1ARCHITECHTURE

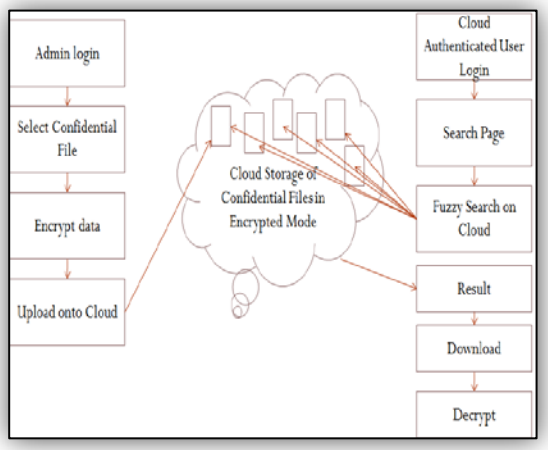

Figure: Flow diagram

The work flow diagram describing the flow of project that how it get work logically. The diagram includes all important term related to our project. In the given diagram we provide login for admin that

ISSN 2348 – 7968

is the authorized user have all rights to see and update all confidential data store on cloud.

In the given diagram we show to main steps and how it gets process in our project. Uploading file and another one is to search file by using keyword.

The first one is u First for uploading file on cloud , admin need to login then admin select file which he want to upload, after that the system perform encryption on file the system finally upload the file on cloud and store in it.
Another one is to search the file on cloud by using fuzzy concept for search, also the user needs to login first then type keyword for search .Now the system searches file on cloud and decrypt the file and show to the result to user.

4. APPLICATIONS

We can use this concept in following domains…
A. Matrimonial Domain
Matrimonial companies need to maintain cloud of resumes with secrecy of data as well as they need that their requirement will match in encrypted data.
B. Banking Sector
Banking sector has maintained data of its customers in encrypted mode to maintain privacy of data. They also need to search from confidential data.

5. CONCLUSION

In this paper we want to apply the fuzzy concept to autocorrect the misspelled words so that it becomes easy to access the application.
Hence, we can conclude that we are developing this application to upload documents with encrypted mode and searching results from files using fuzzy search concept. Result will be decrypted and displayed in decrypted format.

This app can be used in every department where confidentiality of data is very important and searching from encrypted data can be done.

6. REFERENCES

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYP'04, 2004

[2] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proceedings of Crypto 2007, volume 4622 of LNCS. Springer-Verlag, 2007.

[3] Google, "Britney spears spelling correction," Referenced online at http://www.google.com/jobs/britney.html, June2009.

[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00,2000.

[5] E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, Report 2003/216, 2003, http://eprint.iacr.org/.

[6] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an encrypted and searchable audit log," in Proc. of 11th Annual Network and Distributed System, 2004.

[7] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS'05, 2005.

[8] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS'06, 2006.

[9] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. of TCC'07, 2007, pp. 535-554.

[10] F. Bao, R. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings,"inProc.