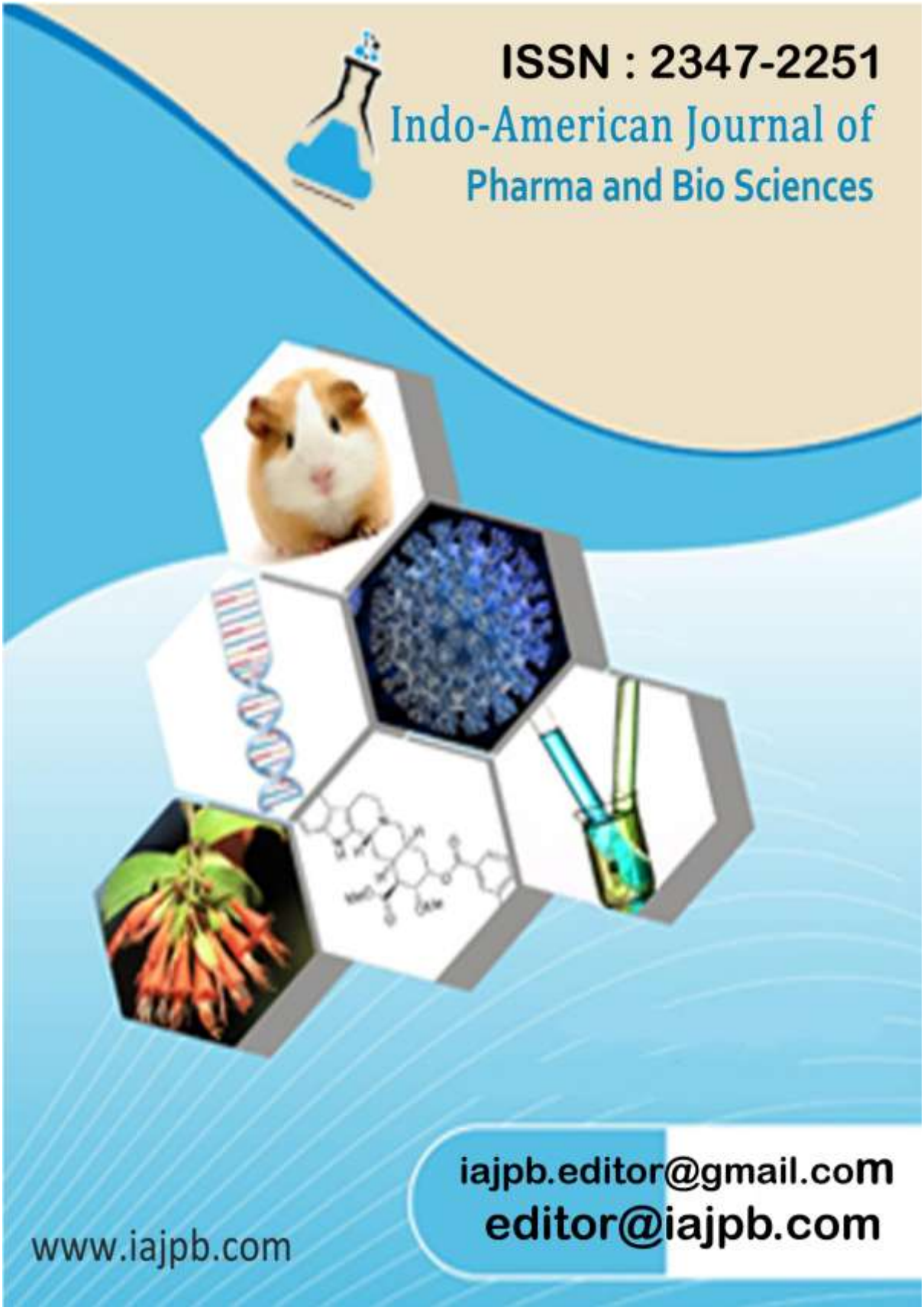
ISSN : 2347-2251
Indo-American Journal of
Pharma and Bio Sciences
iajpb.editor@gmail.com
editor@iajpb.com
www.iajpb.com

Indo-American Journal of Pharma and Bio Sciences

Vol. 9, Issuse 4, Nov 2021

A MOBILE CLOUD BASED APPLICATION FOR ENCRYPTED DATASEARCH ACROSSUSINGTES

Shashidharani Vaddineni1HanyEldeib2

Abstract:Data privacy is a big issue that prohibits people from keeping files on the cloud, which is convenient and inexpensive. Encrypting files before uploading them to the cloud and decrypting them after they are accessed is one technique to improve data privacy. Encryption of data is a challenging operation for mobile devices, and retrieval of data is a demanding procedure involving connection between a user's device and a cloud service. These concerns may add a significant amount of computing overhead and resource consumption for mobile device users, making encrypted search over the mobile cloud a tough and challenging activity for the user to perform. In this study, we have introduced TEES, a mobile cloud-based encrypted search system that uses more bandwidth and consumes less energy. To improve mobile client-cloud communication, the suggested architecture would relocate computing from mobile devices to a cloud server. Storage on the Go, Searchable Data Encryption, Energy Savings, and Congestion Reduction

I.**INTRODUCTION**

Using a cloud storage system, customers have access to their data while it is stored, managed, and backed up remotely on the cloud. A large quantity of data can be saved in Mobile Cloud Storage [1], [2] and even serves as the primary file storage for mobile devices [3]. It is possible to save and retrieve files or data on the cloud via a wireless communication, which improves the data availability of the file sharing process without draining the mobile device resources [4]. When sensitive data is sent to the cloud, the owner encrypts it and the data user retrieves it using an encrypted search strategy. The data privacy issue is paramount in cloud storage systems. In the cloud, mobile

Traditional data encryption methods are employed in MCS [5], [6]. New issues arise when a mobile cloud storage system is used, due to the restricted computing and battery power of a mobile device. As a result, MCS requires an effective encrypted search mechanism. That's why for mobile cloud storage apps, we came up with an architecture called TEES (Traffic and Energy saving Encrypted Search). TEES fulfills the capabilities of the encrypted search platform invoked in cloud storage systems by altering the ranking keyword search.

VirginiaInternationalUniversity

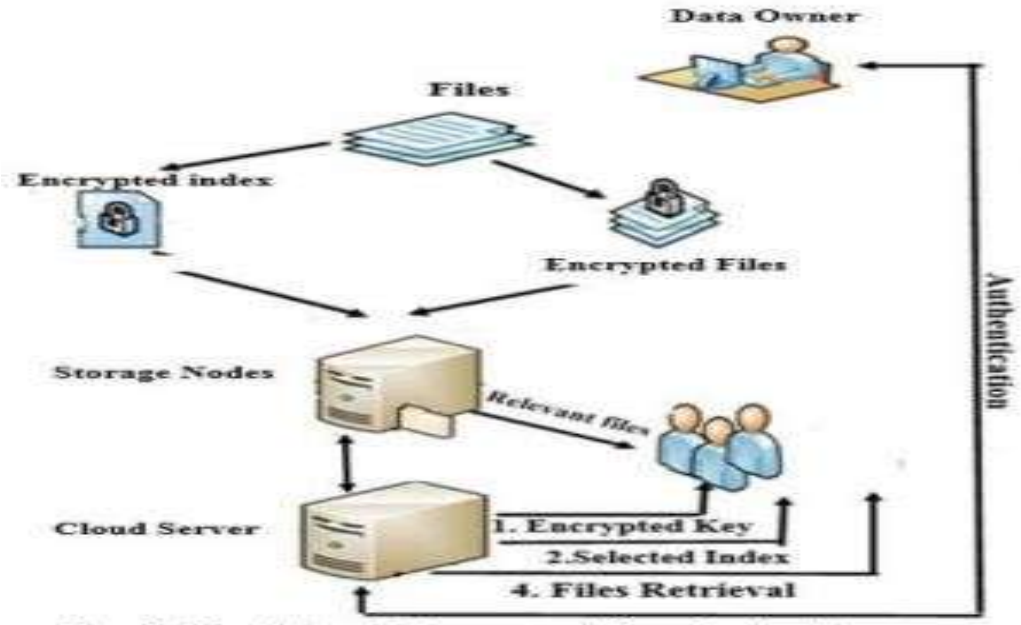

Fig. 1. Traditional Encrypted Search Architecture

Encrypted Search Methods In the last few years, encrypted search has grown to include data sharing that protects user privacy. One technique [7] suggested encrypting a document's words one at a time. As a result, it is not compatible with existing file encryption systems, and it cannot handle data that has been compressed in size. Following that, a slew of new techniques for encrypted search tactics emerged, including Term Frequency-Inverse Document Frequency is a technique used in information retrieval. [8]. Boolean and ranking keyword search are the most commonly used methods of encrypted searching. In a Boolean keyword search, the server returns files based on whether or not the keywords appear [7, [9], [10]], without considering the relevance of those terms.

2. The most popular search terms A keyword search was built by Chang et al. [11], however it was not able to return the most important files. OPE was used to encrypt the file set in the older systems. Agrawal et al. [12] implemented one-to-one mapping in their most recent study.

OPE, which will result in the loss of statistical data. Control. An OPE with a one-to-many mapping was implemented by Wang et al. For security reasons, they came up with a complicated algorithm. However, because their method was complicated and required a large amount of computer power, they would have a problem with both their productivity and their energy usage.

III.**TEESSYSTEMDESIGN**

• We propose a new architecture called TEES to allow an encrypted search technique with a higher level of security for cloud data. It was our goal to provide a secure, encrypted search solution for mobile cloud storage based on some threats. We initially introduced the design idea, and then we developed our own protocols for searching and improving cloud data using our own algorithms. The security and objectives of our plan are met. THE ESSENTIAL CONCEPT OF TEES

• With TEES, the appropriateness scores will be calculated and ranked in the cloud. A low-power design strategy that relies on outsourcing compute applications to the cloud has been discovered. In order to reduce the quantity of calculations performed by mobile systems and save energy, cloud providers can give compute cycles that can be used by users. Offloaded applications, on the other hand, aim to increase the amount of transmission and consequently the amount of energy consumed. To verify the data users, the data owner employs the process of verification. • There are usually three basic processes:

• The data owner encrypts the file sets and its index during the preparation and indexing stages before storing them in the cloud..
• In the search and retrieval procedure, the data user sends a request to the cloud server to search for files based on a keyword. On to how TEES tackles power efficiency and security issues when altering these processes, now that we've introduced the concept. i. New Search and Retrieval Methods The data (see Fig. 2).

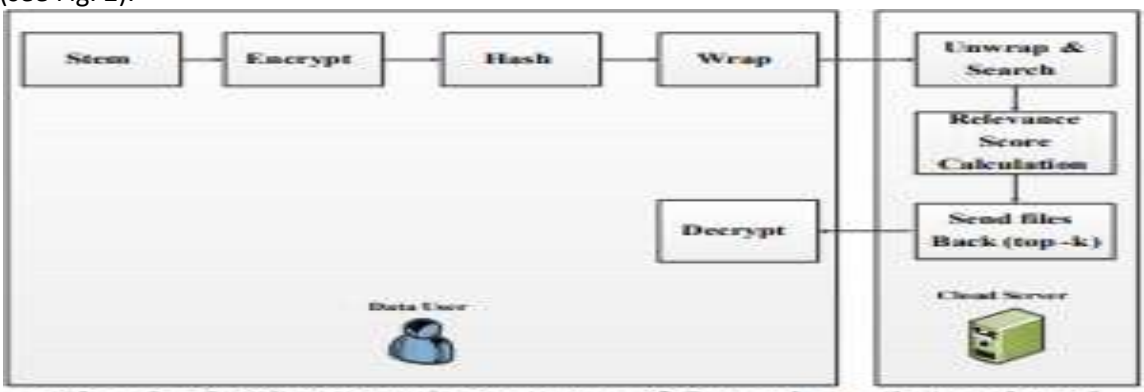

Fig. 2. ORS: Novel Process of Search and Retrieval

i)If a data user wants to receive the top-krelated files based on a keyword then, theyfirstobtainauthenticationfromthedataowner and then receives the key to encryptthekeywords.
ii)The data user branch the keywords to beinquireand encrypts itusingthe keys.
iii)Thedatauserwrapstheencryptedkeywordint oatuple,includingsomenoisetoremove statistic information loss. Then, it issend to the cloud server together with thenumberk.Thewrapmethoddeliversthean attacker's secret identity First, the cloud server verifies that the user has the proper permissions to access the wrapped keywords. In cases when the data owner has provided the server's address, a search is conducted and an alert is displayed. In the mobile client, the data user decrypts these files and retrieves the original data.

EFFICIENCY OF POWER AND TRACKING IN IMPROVEMENT

However, these early systems didn't immediately apply to mobile clouds in order to address the specific issue of mobile cloud energy usage. There have been past years where OPE or entirely homomorphic

Techniques for encrypting data [17] and [18] have been recommended. They've proven themselves safe and reliable when it comes to decrypting encoded data. A complicated algorithm isn't appropriate for mobile devices because of the increased need for power usage. TEES uses an order-preserving encryption algorithm because this is the easiest to implement. The importance of energy and performance in mobile cloud computing was raised by Kumar et al. [14]. According to their findings, there are four fundamental techniques to saving energy and extending the battery life of mobile devices.

APPLICATIONA.TEES Cloud Security Enhancement Implementation Modified routines and new algorithms are used to implement the modules in TEES so that security can be improved while also reducing energy and traffic use. There are three phases to our system's introduction. Using OPE to encrypt a TF table will allow the data owner to offload the calculation and ranking burden on therelevancescorestothecloud.Soastocontrolt he statistics Our one-to-many OPE in the data owner module was enforced to prevent data leakage. Additionally, we added additional noise to the data module to help deal with the loss of keywords-files.. We developed a cloud-based ranking system to determine the significance of the top-k files. The Data Owner owner receives a TF table as an index and encrypts it using OPS (Order Preserving Encryption) during the preprocessing and indexing steps. Therefore, the cloud server can calculate and rank the relevant scores without having to decode the index. This ensures that the unloading of the estimated load is safe and feasible. This is how TEES' new search and retrieval methods work

Module's of energy and performance in mobile cloud computing was raised by Kumar et al. [14]. According to their findings, there are four fundamental techniques to saving energy and extending the battery life of mobile devices.

APPLICATIONA.TEES Cloud Security Enhancement Implementation Modified routines and new algorithms are used to implement the modules in TEES so that security can be improved while also reducing energy and traffic use. There are three phases to our system's introduction. Using OPE to encrypt a TF table will allow the data owner to offload the calculation and ranking burden on therelevancescorestothecloud.Soastocontrolt he statistics Our one-to-many OPE in the data owner module was enforced to prevent data leakage. Additionally, we added additional noise to the data module to help deal with the loss of keywords-files.. We developed a cloud-based ranking system to determine the significance of the top-k files. The Data Owner Module's re-design By using one-to-many OPE, we were able to control the loss of statistical information by customizing the index construction method. To maintain TEES's security, the authentication process between the data owner and the data user has been strengthened as well..Many researchers are currently working to improve the efficiency of encrypted search with multi-keyword ranking. Using a one-way search, Wang et al. were able to decrypt the encrypted data. Because of this, it is important to note that multi-keyword ranked searches could have a more serious problem with the loss of association between keywords and files. Attackers could use wireless communication channels for mobile cloud to learn about correlations between keywords and files. For multi-keyword encrypted search, Cao et al. created a privacy-conserving technique with a way to limit the "double key loss." The fuzzy search technique was provided in a multi-keyword fuzzy context, however it suffers from erroneous search time and two round-trip communications [19]. Multi-keyword search is likely to become the standard encrypted search method in the future, but it is now the subject of ongoing study.cannot offer a genuine method. Since the single keyword with OPE TF-IDF encryption method will be used to create a more powerful and traffic efficient encrypted data search architecture [19].

V. **GENERAL SYSTEM MODEL FOR THE APPLICATION**

File/IndexEncryption:-

PROPOSEDSYSTEM

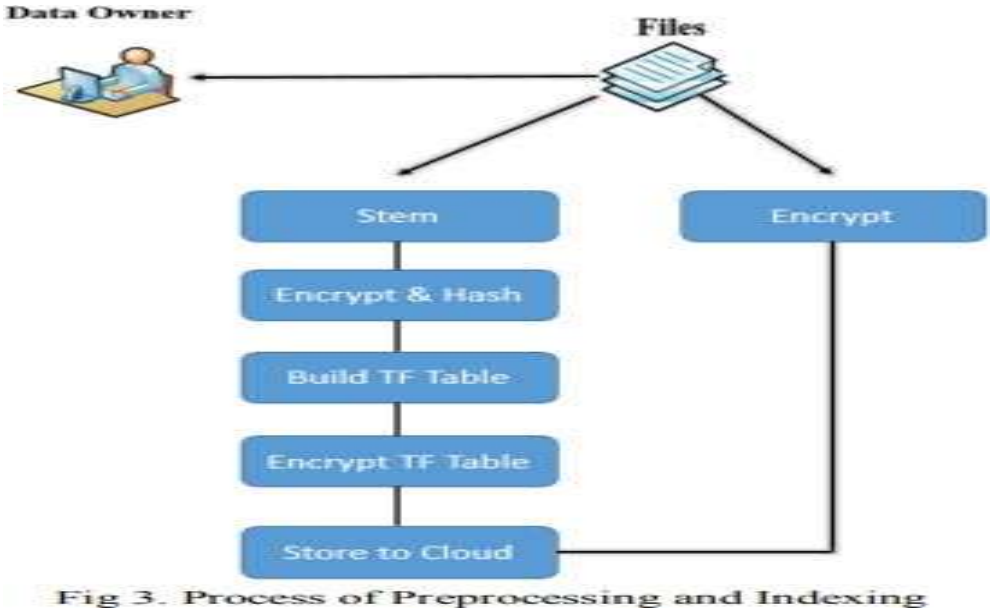

Fig 3. Process of Preprocessing and Indexing

a.Thedataownerfirstexecutesthepreprocessing and indexing work as shownonFigure

1.The owner should convert files that areselected to store on the cloud, for text searchengines[20].
b.Every word in these files goes throughstemming to retain the word stem. Next,
5. **FINAL COMMENTS AND OUTLOOK** In this study, we present a new architecture, TEES, as a first step toward developing a mobile cloud storage-based encrypted keyword search engine. Starting with a simple approach that we tested against earlier encrypted cloud search tools, we demonstrated their lack of efficiency in a mobile cloud environment. This method is more time and energy intensive, but it saves a significant amount of energy when compared to other methods that achieve the same level or better of security. On the basis of TEES, this work can be extended to include further unique implementations. To enable the search of encrypted material, we've devised a single term search technique. However, we haven't ruled out future iterations of our current project. In order to execute encrypted data search on mobile cloud in the future, we intend to offer a multi-keyword search system. REFERENCES\s[1] It is time for a break in the clouds: toward a definition of cloud computing, according to L. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner in the ACM SIGCOMM Computer Communication Review.

Knowledge Discovery and Data Mining, Springer, 2012, pp. 257–263. Yu and Q. Wen "Design of a security solution for mobile cloud storage."
IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011: D. Huang, "Mobile cloud computing."
Is storage acquisition having a negative impact on performance?Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, IEEE, 2012, pp. 646–653, discusses the relative cost-effectiveness of private and public cloud storage. [5] "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing, J. Oberheide, K. Veeraraghavan, E.

thedataownerencryptsandhasheseverytermto fixits entryin theindex.
c.Theindexisthencreatedbythedataowner.Finally,thedataownerencryptsthe
The cloud server indexes and saves the encrypted file set on the cloud.
Cooke, J. Flinn, and F. Jahanian. At the ACM in 2008 (pg. 31–35).
Journal of the ACM, "When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenged in Mobile Environments," Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, June 2006. Pages 43–48 in ACM, 2010. ACM, 2010.
« Practical techniques for searches on encrypted data », in S&P 2000 (Security & Privacy), Song, Wagner & Perrig [7]. Proceedings. IEEE, 2000, pp. 44–55; IEEE, 2000.
In Applied Cryptography and Network Security (Springer, 2004), p. 31–45: P. Goll, J. Staddon, and B. Waters "Secure conjunctive keyword search over encrypted data."
Reference
Key encryption with keyword search, in Advances in CryptologyEurocrypt 2004, Springer, 2004, pages 506–522, by D. Boneh et. al., G. Di Crescenzo, R. Ostrovsky, and G. Persiano.
10] R. Curtmola, J. Garay, S. Kamara, and J. Platt
Refined definitions and efficient constructions of "searchable symmetric encryption" appear in Proceedings of the 13th ACM Conference on Computer and Communications Security (ACM), pp. 79–88 in ACM, 2006.
Y.In Applied Cryptography and Network Security, Chang and Mitzenmacher, "Privacy preserving keyword searches on remote encrypted material," Published by Springer in 2005 (pp. 391–421).
In Proceedings of the 2004 ACM SIGMOD international conference on Management of data, R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," From 563–574 in ACM, 2004.
[6] IEEE Transactions on Parallel and Distributed Systems, Volume 23, No. 8, August 2012, Pages 1467–1479. Enabling

secure and efficient ranked keyword search across outsourced cloud data
[7] To save energy, you may want to consider using the cloud if you use a mobile device. Computer, vol. 43, no. 4, p. 51–56, October 2010.
[8] A. Boldyreva, Y. Lee, and N. Chenette
[9] At the EUROCRYPT 2009 conference in 2009, A. O'neill presented his work on "Order-preserving symmetric encryption."
[10] In Advances in Swarm Intelligence, 2012, J. Zhang, B. Deng, and X. Li created an encrypted document rating system based on additive order-preserving encryption.
[11]PhD dissertation by C. Gentry: "A completely homomorphic encryption system," Stanford University, 2009;
[12]Advances in Cryptology-ASIACRYPT 2010, 377–394 (Steinfeld and Steinfeld, "Fast Fully Homomorphic Encryption") (October 2010)
[13]On the Mobile Cloud, an Efficient Search Scheme over Encrypted Data is presented in IEEE/ACM Transactions on Cloud Computing.
[14]Text search engines can benefit from inverted files, according to J. Zobel and A. Moffat. Surveys by ACM Computing(CSUR), vol.38, no.2, p.6, 2006.