Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY
Full Length Article

Energy Efficient Search Scheme Over Encrypted Data On Mobile Users On Cloud

V.Premnath [a], M.Mohammed usman [a],K.Karthick kumar [a], M.Vetrivel [b]

[a] *Student , Department of IT, K.S.Rangasamy College Of Technology,Tiruchengode, Tamilnadu, India*
[b] *Assistant Professor , Department of IT, K.S.Rangasamy College Of Technology,Tiruchengode, Tamilnadu, India*

***Corresponding Author**
M.Vetrivel

ABSTRACT: Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging In this work, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval, meanwhile the network traffics during the file retrievals are also significantly reduced.

1 Introduction

Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging

In this work, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval, meanwhile the network

Traffics during the file retrievals are also significantly reduced.

Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, —Pay-as-you-go‖ model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud.

Hybrid Cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Mobile Cloud

In an increasingly connected world, users access personal or shared data, stored —in the -cloud‖ with multiple

devices. Despite the popularity of cloud storage services, little work has focused on investigating cloud storage users‘ Quality of Experience in particular on mobile devices. Moreover, it is not clear how users‘ context might affect QoE. We conducted an online survey with 349 cloud service users to gain insight into their usage and affordances. In a 2-week follow-up study, we monitored mobile cloud service usage on tablets and smart phones, in real-time using a mobile based Experience Sampling Method (ESM) questionnaire.

We collected 156 responses on in-situ context of use for Drop box on mobile devices. We provide insights for future QoE-aware cloud services by highlighting the most important mobile contextual factors (e.g., connectivity, location, social, device), and how they affect users‘ experiences while using such services on their mobile devices. These devices offer a vast range of new affordances to users and enable connectivity anywhere, at any time and from any device. However, one unyielding disadvantage of these lightweight, mobile devices is their limited storage capacity, which also limits their possible uses. It is also more common to find services and applications that work across different mobile devices and platforms. As a result, the related user behavior and usage patterns have become more complex and a range of problems has emerged. One recurring challenge is to connect multiple devices that have vastly different characteristics and requirements and how to synchronize the stored data across these devices in an effortless way. With recent improvements on network speed, reliability and increased availability, and based on principles of cloud computing, a growing number of consumer market and business-oriented providers of cloud storage have started to address these and other challenges. In spite of the controversy surrounding the notion of ‗cloud computing‘ and whether it is really new or just a new wrapping , cloud computing is (re-)shaping the Internet and the services it provides. Infrastructure and scalability management are hidden away onto the ―cloud.‖ Services such as Amazon‘s Elastic Compute Cloud, Microsoft‘s Azure and Google‘s App Engine provide ―flexible‖ hardware and storage availability in a cost effective approach. Currently, Drop box is one of the most popular cloud computing services, available on desktop and mobile environments. It offers almost unlimited cloud storage on the go, given the availability of Internet connection (except when accessing cached files). Files can be easily accessed and automatically synchronized across a range of devices: laptops, smart phones, and tablets. Over the last decades, increased attention was given to the world of technology users/society, the actual use and the meaning of technology (e.g., in research, policy and practice). Especially in the context of ICT research and innovation, there has been a growing awareness that users and consumers are demanding, powerful, and self conscious stakeholders that cannot be simply ignored. In various research fields (e.g., HCI, telecommunications, multimedia and vision research, service management) an effort is being made to measure and understand how users experience ICT products, applications and services. Traditionally, emphasis was put on technological excellence and quality. Since the 90‘s however, experiences rendered through the encounters with a product, brand, service or application, have notably been emphasized as a basis for differentiation. The quality of users‘ experiences have been linked to market success or failure of new and existing products, applications, services. This renewed focus on experience is reflected in the literature by relatively young concepts such as User Experience, Quality of Experience and Customer Experience, which stem from distinct disciplines and research traditions, but which nevertheless have some common grounds. We must acknowledge that experiences are subjective, individual and highly complex and therefore it is necessary to investigate them from a multi-disciplinary perspective and through involvement of actual users. Other unknown factors may influence users‘ experiences and should therefore be investigated and better understood. ‗Quality of Experience‘ has its roots in the field of Telecommunications, but over the last decade it has also acquired a more prominent role other fields and disciplines. A more holistic and broadly supported perspective on QoE was introduced, defining it in terms of affective states, as the: ‗degree of delight or annoyance of the user of an application or service. It results from the fulfillment of his or her expectations with respect to the utility and / or enjoyment of the application or service in the light of the user's personality and current state.

Cloud Storage

Cloud computing is a hot topic in recent research and applications. Because it is widely used in various fields. Up to now, Google, Microsoft, IBM, Amazon and other famous co partnership have proposed their cloud computing application. Look upon cloud computing as one of the most important strategy in the future. Cloud storage is the lower layer of cloud computing system which supports the service of the other layers above it. At the same time, it is an effective way to store and manage heavy data, so loud storage attract some researchers. Therefore, the research of cloud storage will not only follow trends, but also has a high application value. Cloud storage is a distributed file system with complicated architecture. Firstly, it is implemented on top of the cloud computing infrastructure which is based on cheap, virtualized and unreliable physical hardware, Secondly, it supports large server scale, and has efficient heavy data storage. For all of these challenge, the key technologies of the system architecture and modules design is Cloud storage.

This article discusses the background of the development of cloud storage, gives the definition of cloud storage, describes the characteristics of cloud storage, and proposes the mode of cloud storage architecture. Exposing the key technology of cloud storage systematically and comparing functions of different storage software. Cloud computing has become one of the hottest terms of the 21st century emerging technology, and cloud computing relate to a variety of themes occupy the main status of the mainstream media, there are a variety of books on cloud

computing has also been to shelves in recent years. Cloud storage is derived from the concept and practice of cloud computing. Through the personal application like Drop box, I Cloud, Google Drive, it coming into people‘s live, effectively changed the people's understanding of the storage, improved the way files are stored.

Internet makes the world accessible. Cloud storage is the key infrastructure to achieve seamless information sharing and service interaction experience from different users, different applications, different devices around the world. It will become a new public infrastructure service, like water, electricity, available in anytime, anywhere. The features of high performance, high flexibility, high capacity and high security will make cloud computing and cloud storage become the cornerstone of the future of internet innovation. At the same time it makes distributed database, mobile computing, search technology, Internet of Things and other technologies developed, and increase the user experience. In order to provide data storage services, cloud storage employs software to interconnect and facilitate collaboration between different types of storage devices. Compared to traditional storage methods,cloud storage poses new challenges in data security, reliability, and management.

This work introduces four layers of cloud storage architecture: data storage layer connecting multiple storage components, data management layer providing common supporting technology for multiple services, data ser-vice layer sustaining multiple storage applications, and user access layer. It then examines a typical cloud storage application—backup cloud (B-Cloud), and discusses its software architecture and characteristics. Cloud computing is a hot topic in recent research and applications. Up to now, Google, Microsoft, IBM, Amazon and some other famous companies have proposed their cloud computing application, and put cloud computing as one of the most important strategy in the future. Cloud storage is the lower layer of cloud computing system which supports the service of the other layers above it. In addition, it is an effective way to save and manage heavy data. So it focused even more attentions from some researchers. The definition of cloud computing can be traced back to 1961. The famous American computer scientist John McCarthy who is the winner of the Turing Award put forward the concept of the cloud computing. He though that the computing power could be used by users like water, electric, gas or other public resource. However, for a long time, this idea has only stay in the dream stage. Until the beginning of the 21st century, this idea has been known with the development of technology and the maturity of the application and 2010 is the first year of real cloud era.

Amazon introduced the Elastic Compute Cloud. The major equipment manufacturers and service providers have also launched on demand utility computing (utility computing is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate.) and other similar computing services. The definition of cloud storage is still not very accurate, many people think that cloud storage is the network disk like Dropbox, Google Drive. But the network disk is just one of the forms of the cloud storage which is the closest expression to the public. It stores the user's file data to the network that achieve data storage and backup. It meet user‘s purpose of data storage, using, sharing and protection. Some people think that cloud storage is a kind of document network storage, such as Ever note notes storage services. Many people think the cloud storage is a system device to provide data storage and business access functions.

The device is achieved through the cluster applications, network technology or distributed file systems and other functions. Cloud storage doesn‘t have the authoritative definition of the industry, but the industry has reached a basic consensus on the cloud storage. Cloud storage is not only a storage technology or equipment, but also a service innovation. The definition of cloud storage should have the following two parts. First one is that in the service-oriented aspects of the user, it provides on-demand service application model, users can connect to the cloud through the network, to save user‘s data in cloud storage anytime, anywhere. Secondly, in terms of build cloud storage service, it achieves massive, resilient, low-cost, low-power shared storage re-sources through the distributed, virtualized, intelligent configuration and other technologies.

The contents of IaaS and SaaS are not the same. From the perspective of IaaS, cloud storage provides a service for data storage, archiving, and backup. From the SaaS point of view, cloud storage service is very diverse the service has online backup document notes save network disk business photo preservation and sharing home video. Just like the IaaS business to provide cloud storage. Service providers like Amazon's S3, however, there are more cloud storage provider try to sell the SaaS business, such as Ever note and Google Docs.

A Secured and Searchable Encryption Algorithm For Cloud Storage

Cloud computing is a new generation technology which efficiently support the client oriented services. Now in these days there are a number of applications which consumes the cloud storage service for storing and retrieving information. In such conditions the data owner management and privacy preservation cryptographic techniques are utilized frequently. But due to cryptographic technique of security implementation the data leave their own format and converted into other unreadable format. Due to this retrieval of required information becomes complex. Therefore in this paper a proposed solution incorporate the hash table management and indexing techniques to keep track the actual data contents in terms of document features which may help for encrypting user data and identifying the user data and privacy**.**

The Internet access becomes available in the recent years, Cloud computing is an internet based technology; it is

using hardware and software as computing resources to provide service through internet. Cloud computing is being widely used now-a-days enabling the end user to create and use software from anywhere at any time without worrying about the execution of the technical information. Cloud computing technology provide unlimited resources and services like data storage service which helps to manage the user data. Now a days, with the help of dynamic data operation with computation user can store their data in cloud. Which makes the copy of data for further updating and verification of the data loss. Here with the help of cryptographic technique data can be secured from unauthorized user or access. The benefits of the cloud storage are flexible with reduced cost and they also manage the data loss risk and so on.

To provide an information retrieval function while addressing the security and privacy issues, the concept of searchable encryption was introduced in an earlier study.With searchable encryption, the entity performing the retrieval service is not allowed to learn the content of the queries and responses. Instead, some additional encrypted index terms (serving as keywords or hints) are used for the data search process. The entity uses a cryptographic algorithm similar to decryption for finding the correspondence between the encrypted query and the encrypted data content. They summarize the essential requirements specified in for searchable encryption in terms of privacy and security issues from the view point of unqualified users as follows:

Privacy of data: No one can uncover information about data content from the query and response as well as the cipher text itself.

Privacy of the data owner: No one can learn about the identity of the data owner from the encrypted content. they suggested that one‘s identity can be viewed as a combination of several attributes expressing the characteristics of the user in the form of access policy by using Boolean expressions such as AND, OR, or NOT. On the other hand, CP-ABE is complementary to KP-ABE by enabling encrypt or to specify access policy combined with the cipher text. Both schemes allow secure one-to-many communications such as targeted broadcasts for a specific group and individual user according to their attributes, some studies suggested modification of ABE schemes by hiding the access policy. These schemes operate on the assumption that the data owner directly delivers the cipher text to the receiver without an intermediate third party. In other words, when adopting those approaches directly in cloud storage, decryption keys can be exposed to an unauthorized third party. Hence, they are not feasible for data retrieval services in the cloud storage systems because the test procedure allows the CSP to learn which attributes the user has. motivate and solve the problem of supporting effective ranked keyword search for providing efficient use of remotely stored encrypted data in Cloud. They firstly give a fundamental scheme and show that by same existing searchable encryption method, it is not efficient to achieve ranked search. So they appropriately weaken the security guarantee, to solve this security problem they developed cryptography first OPSE, and derive an efficient one-to-many order-preserving mapping function, which allows the effective RSSE to be designed. Through thorough security analysis, they show that their proposed solution is secure and maintain the privacy, while correctly realizing the aim of ranked keyword search. And also shows that their solution enjoys ―as-strong-as possible‖ security guarantee compared to conventional SSE schemes, Note that in their design, they focus on single keyword search.

This section includes involved work and identified issues in system in addition to that an optimum solution is also provided. The cloud environment provides support for efficient computing and enables to provide the storage solutions at the remote end. The main aim is to address the following issues in the existing cloud storage:

1. Data security: The data is placed on the cloud which is not much secured due to third party access and treads therefore the data security in cloud storage is required

2. Data owner and client privacy management: The data owner and client in not distinguishable using the data additionally the privacy on such data is access is required.

3. Searchable data space: The cryptographic manner of data security converts the formats and not a bit of data recovered during the information retrieval. In this paper we discussed various method of searchable encryption to secure the data in cloud storage. Also we discussed about cryptography methods which helps to convert the data from readable to unreadable form so our data could be saved in cloud storage from adversary. By studying all these paper we can conclude that the essence of security for cloud storage is very necessary so that client could feel secure while accessing the cloud storage services. In this work we proposed a scheme for secure data accessing with maintaining its privacy by using strong cryptographic algorithm. Our future work will attempt to enhance the feasible solution.

2. Proposed system

In order to achieve security enhancement with energy and traffic efficiency, we implement the modules in TEES using modified routines and new algorithms. Our system will be introduced in three parts. As previously mentioned, the data owner should build a TF table as index and encrypt it using OPE in order to offload the calculation and ranking load of the relevance scores to the cloud. So as to control the statistics information leak, we implement our one-to-many OPE in the data owner module. We also wrap the keywords to be searched by adding some noise in the data user module to help controlling the keywords-files association leak. In order to get top-k relevant files, we implement a ranking function to calculate the relevant score on the cloud. Given a keyword in ORS, the cloud server is in charge of calculating the relevance scores for the data user to get the corresponding top-k relevant files. Therefore, we implement both the unwrap and rank functions in the cloud server module. Hence these modules are modified compared with the traditional ones.

3. In STAMP Enabled TEES, the cloud server calculates the relevance score and finds the most relevant files corresponding to a given keyword. In order to find the TF value of a queried keyword, the cloud server should also know the unwrap function of the user-supplied wrapped tuple. Therefore, the cloud server gets more information than any potential attacker. Therefore, a curious cloud server may determine the terms queried by the users only by comparing the queries and the results. As most of the previous schemes, we assumed that our test cloud server semi-trusted, and therefore we only need to minimize the amount of information it acquires. Moreover in terms of performance improvements, information leakage does not seem to be a very serious problem, and updating the TF table periodically also
protects the index from being inferred by the server.

4. Note that TEES is established with widely used TFIDF encryption approach, and all nature defects of this encrypted search scheme cannot be completely resolved even TEES In addition, when a data user performs a search, the keyword to be queried will be encrypted by the data owner‘s key. The user receives a hash table after the first time it is authorized by the data owner. In order to prevent these users from running secret searches maliciously.

File Search and Retrieval Time

We compare the File Searching and Retrieval Time (FSRT) for the three schemes in this subsection as illustrated in Figure 10. We test the FSRT for different files with size ranging from 100KB to 1MB. We observe that the FSRT of PTS is the shortest since it does not have to perform any security computation. The FSRT of ORS is effectively reduced when compared to the one of TRS. This difference is due to the advantages of the TEES design in terms of relevance score calculation offloading, and thus leads to reduction of file search and retrieval process. The FSRT value of ORS is very near to the one of PTS, implying a very low cost to security on the mobile device. For example, TEES saves FSRT by 46% compared to TRS for files of size 100KB, and by 23% for 1MB files .The file retrieval time only depends on the file size and network bandwidth. When offered a greater bandwidth, TEES becomes more efficient since downloading time of files becomes a bottleneck of other schemes. The decryption time of the files is equal in all schemes and it is therefore pointless to measure it.

FSRT analyse of PTS, TRS and ORS

The efficient FSRT of TEES is achieved by improving the process efficiency, since only a single round of communication and relevance score calculation offload are used. The searching process is analysed in Table 1. Without any security service, PTS (Plain Text search) does not spend any time on stemming and encryption; neither does it on hash and wrap. On the other hand, ORS and TRS provide encrypted search schemes with related overhead. As shown in Table 1, ORS can improve the ―request/response‖ time significantly than TRS from 370ms to 190ms (saving 180ms), and eliminate the ―client file search‖ time by offloading it onto the server (saving 260ms). Notice that the ―sever file search‖ calculation workload of ORS is 75ms, which is 5ms longer than that of TRS. This is explained by the fact that the server takes the offloaded search calculation of the mobile user. In the other words, TEES eliminates the ―client file search‖ time at the cost of a little heavier ―server file search‖ time. This proves that the offloading is highly efficient (5ms vs. 260ms). Moreover, ORS spends more 5ms on wrapping the hash value than TRS for enhancing the security. Note that the ―server file search‖ time of PTS is higher than the other two schemes, since the server should execute stem and hash function for plaintext file search, while the hash functions are executed by the mobile data user in both TRS and ORS. Overall, ORS is secure and effective.

Throughput

The calculation offload from the mobile device to the cloud data center reduces the execution time of the relevance score calculation due to the higher server capacity. Therefore, this also greatly increases the system throughput besides FSRT improvement; We observe that the file access acceleration is very effective when dealing with small files as the relevance score calculation is executed more frequently. For example, on a 100KB file, the access speed is increased from 104KB/s to 194KB/s, almost doubling the throughput. The acceleration is still effective when accessing files with size 1MB (29.6% acceleration). The throughput of ORS is not much less than that of PTS.

Implementation to achieve an encrypted search in a mobile cloud. The security study of TEES showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. TEES is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Based on TEES, this work can be extended to more other novel implementations. We have proposed a single keyword search scheme to make encrypted data search efficient. However, there are still some possible extensions of our current work remaining. We would like to propose a multi-keyword search scheme to perform encrypted data search over mobile cloud in future. As our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency.

3.Conclusion

In this work, we developed a new architecture, TEES as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. We started with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and showed their inefficiency in a mobile cloud context. Then we developed an efficient

implementation to achieve an encrypted search in a mobile cloud. The security study of TEES showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. TEES is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Based on TEES, this work can be extended to more other novel implementations. We have proposed a single keyword search scheme to make encrypted data search efficient.

References

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, ―A break in the clouds: towards a cloud definition,‖ ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] D. Huang, ―Mobile cloud computing,‖ IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[3] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, ―Virtualized in-cloud security services for mobile devices,‖ in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[4] J. Oberheide and F. Jahanian, ―When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,‖ in Proceedings of the Eleventh Workshop on Mobile Computing Systems ACM, 2010, 43 48.

[5] A.Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.

[6] D. Song, D. Wagner, and A. Perrig, ―Practical techniques for searches on encrypted data,‖ in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44– 55.

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ―Public key encryption with keyword search,‖

[8] in Advances in Cryptology- Eurocrypt 2004. Springer, 2004, pp. 506–522.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ―Searchable symmetric encryption: improved definitions and efficient constructions,‖ in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[10] Y. Chang and M. Mitzenmacher, ―Privacy preserving keyword searches on remote encrypted data,‖ in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.

[11] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, ―Zerber+ r: Topk retrieval from a confidential index,‖ in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449.

[12] C. Wang, N. Cao, K. Ren, and W. Lou, ―Enabling secure and efficient ranked keyword search over outsourced cloud data,‖ Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[13] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ―Privacy-preserving multi-keyword ranked search over encrypted cloud data,‖ Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[14] J. Zobel and A. Moffat, ―Inverted files for text search engines,‖ ACM Computing Surveys (CSUR), vol. 38, no. 2, p. 6, 2006.

[15] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, ―Order preserving encryption for numeric data,‖ in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[16] D. M. Blei, A. Y. Ng, and M. I. Jordan, ―Latent dirichlet allocation,‖ the Journal of machine Learning research, vol. 3, pp. 993–1022, 2003.

[17] Q. Chai and G. Gong, ―Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,‖ in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922.

[18] S. Kamara and K. Lauter, ―Cryptographic cloud storage,‖ in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[19] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, ―Toward privacy assured and searchable cloud data storage services,‖ Network, IEEE, vol. 27, no. 4, pp. 56–62, 2013.

[20] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ―Privacy-preserving multi-keyword ranked search over encrypted cloud data,‖ in

[21] INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 829–837.