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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

An Efficient Seek Scheme over Encrypted Statistics on Mobile Cloud

Nagamani P H [1], Jyothi R [2], Monisha C[3], ChaithraG [4]

U.G Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, Karnataka, India[4]

ABSTRACT:Mobile cloud storage may be a provider model at some stage in that data unit of size maintained, controlled and backup remotely on the cloud aspect and within the in the meantime info maintains handy to the consumer over network. To keep info on information garage servers like mail servers and file servers in encrypted type to lessen security and privateness hazard. Encryption and mystery writing unit of measurement overhead for mobile gadgets as a consequences of it's very small and have low computation electricity. TEES (traffic and power competitively priced storage) offloads computation from cell devices to cloud to lessen the capacity intake and know-how stay. Data privacy does not degrade once the performance enhancement ways unit of dimension carried out. The network visitors together drastically decreased at some stage in report retrieval. This paper affords a look at on visitors and energy reasonable seek over encrypted information on mobile cloud.

I. INTRODUCTION

Clouds are a massive pool of easily usable and reachable virtualized resources and offerings. Cloudstorage is a version of on-line facts storage and get right of entry to facts from more than one disbursed and related sources that contain a cloud over community. Mobile Cloud garage (MCS) offers offerings to users to keep and retrievestatistics or documents on the cloud through wi-fi communiqué. MCS is more and more popular on-line service whichfacilitates the report sharing process without draining the local cell tool resources and high records availability. The statistics privateness problem is the maximum important in cloud garage system, so information is encrypted by the proprietor prior to outsourcing on to cloud, and retrieve facts by means of encrypted search scheme. MCS additionally imported many traditional records encryption techniques. However the conventional encryption strategies incurs new demanding situations, in attention of restricted computing electricity, battery capacities, information sharing and getting access to approaches via wireless communiqué. So the design of mobile cloud storage scheme must be green in each electricity consumption and the network visitors with protection necessities through wi-fi verbal exchange. TEES (visitors and electricity efficient seek) introduces architecture to achieve efficiencies of cellular cloud garage utility. TEES employs and modifies ranked key-word search scheme over encrypted records on cellular cloud garage gadget. historically, categories exist for encrypted key-word seek: ranked key-word seek and Boolean keyword search. The ranked key-word search sends top-okay relevant documents to client. The Boolean key-word search sends all of the matching files to the patron, which reasons a larger amount of network traffic. So ranked key-word search is most suitable for the cell cloud storage. The TEES structure with ranked keyword search offloads the security calculation to the cloud to keep strength consumption of mobile gadgets and simplify the encrypted seek procedure to reduce the traffic for retrieving the statistics from encrypted cloud storage. To mitigate the records information leak and keyword-files association leak TEES implements the superior safety scheme for changed search process by way of adding noise in term Frequency distribution feature and retaining Order retaining Encryption attributes.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

II. EXISTING SYSTEM

Look at Of record Retrieval In cellular Cloud garage traditional cloud storage device includes report/ index encryption with the aid of statistics owner then outsource the information to the cloud garage and encrypted seek/retrieval method of the information customers in cloud computing. The statistics proprietor executes the pre-processing and indexing paintings for that he ought to invert documents to store on the cloud for search engines like Google and yahoo as proven in determine every phrase inside the file undergoes stemming to keep the word stem. After that records proprietor encrypt and hashes each word stem. Then data proprietor creates the index and storethe encrypted index in to the cloud with encrypted report set. The records person authenticated with the aid of the data owner for having access to files. The records proprietor assessments the identification provided by using the statistics person and sends the encrypted key again, if the user is a prison person. The hunt and retrieval process are illustrated inside the parent An authenticated user stems the keyword, encrypt with the important thing and hashes to get the index and send the encrypted keyword to the cloud. The cloud server searches for the key-word and send lower back the key-word related index to the person. The user calculates applicable rating with selected index to find the top-okay applicable files to observe up request to the cloud with a view to retrieve files. The location of those documents is selected and despatched again to the data user from cloud server. After thatthe facts user decrypts the document and recovers the unique information. Traditional two round journey scheme is implemented for the authenticated person. This scheme could be very complex and calls for extra computation energy. It is extra complicated than the easy simple text seek scheme, in which looking and retrieving of record is accomplished in a single round experience time without security carrier. The TRS scheme is suitable for the users with non-public computer, however in the case of cell, thecomputation within the person fact incur heavy burden. To solve those issues a novel concept is brought site visitors and power green search.

IV. PROPOSED SYSTEM

The proposed gadget introduces modified algorithms to reap security enhancement with energy and visitors performance. This machine builds inside the components of the information proprietor, information person and cloud server. The facts owner builds the TF table as index, OPE algorithm for encryption. The cloud server implements both unwrap and rank feature. The statistics proprietor is chargeable for building index table, encryption and authentication technique. TF-IDF(term Frequency –Inverse record frequency) is a product of time period frequency and inverse document frequency. The term frequency is the quantity of instances that term happens within the record. The inverse record frequency measures the time period not unusual or uncommon in the complete report. To construct index the data proprietor collects the files to keep in to the cloud. Then extract the phrases from the file, then encrypt and hash the term to shop in to TF table. After that calculate the frequency of term and compute and save the index.OPE (Order maintaining Encryption) technique is used for encrypting the records. This technique makes use of one tomanymapping to map each TF value to a random wide variety in a positive range. This allows saving you the attacker from gathering statistical statistics from the TF desk. The OPE set of rules is quite simple and consumes less electricity. The facts proprietor continues felony consumer set and invalid person set. on the time of authentication facts proprietor assessments the identification of the facts user. If the user belongs to the prison set then information proprietor sends the keys and hash table to the consumer. The data owner exams the international mobile equipment identity of user's mobile and shops its encrypted version. The facts proprietor updates the prison table periodically to ensure the security. The records consumer module executes within the cellular patron facet. The information consumer wraps the key-word using some random quantity after hashing. The wrap feature adds some noise to the key-word to control the keyword-documents association leak. The wrapped key-word sends to the relevance rating calculation to the cloud server. The user decrypts the files similar to the encryption executed via the records proprietor. The authentication function used forthe person authentication. The cloud server unwrap the key-word and searches into the TF table. The cloud server calculates the relevance rankings and returns pinnacle-ok relevant documents to the legal statistics user.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

IV. RELATED WORKS

1. **A break in the clouds: towards a cloud definition**

This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20definitions have been studied allowing for the extraction of a consensusdefinition as wellas aminimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

2.Virtualized in-cloud security services for mobile devices

Modern mobile devices continue to approach the capabilities and extensibility of standard desktop PCs. Unfortunately; these devices are also beginning to face many of the same security threats as desktops. Currently, mobile security solutions mirror the traditional desktop model in which they run detection services on the device. This approach is complex and resource intensive in both computation and power. This paper proposes a new model whereby mobile antivirus functionality is moved to an off-device network service employing multiple virtualized malware detection engines. Our argument is that it is possible to spend bandwidth resources to significantly reduce on-device CPU, memory, and power resources. We demonstrate how our in-cloud model enhances mobile security and reduces on-device software complexity, while allowing for new services such as platform-specific behavioural analysis engines. Our benchmarks on Nokia's N800 and N95 mobile devices show that our mobile agent consumes an order of magnitude less CPU and memory while also consuming less power in common scenarios compared to existing on-device antivirus software.

3.Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient thanall previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We considerthe natural extension where an arbitrary group ofparties other thantheowner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

4. Privacy Preserving Keyword Searches on Remote Encrypted Data

We consider the following problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that you can submit new files which are totally secure against previous queries but still searchable against future queries.

5.Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data

Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

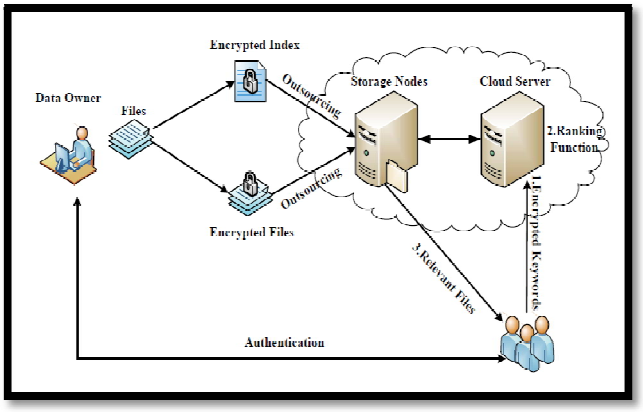
13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitateefficient server-side ranking without losing keyword privacy. Thoroughanalysis shows that ourproposed solution enjoys "as-strong-as-possible" security guarantee compared to previous searchable encryption schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

V. SYSTEM ARCHITECTURE



The general shape of TEES is proven in figure, in which the relevance scores calculation is offloaded to the cloud, which eases the heavy burden on cell customers. Moreover, TEES features only one spherical-journey communications for every are looking for. On this scheme, the documents are looking for and retrieval steps are as follows:

i) The facts user sends his identity to the factsproprietor and get the call of the sport keys if authenticated.

ii) An authenticated consumer stems the keyword to be queried, encrypts it with the keys and hashes it to get its access within the index. Then the encrypted key-word is dispatched to the cloud server.

iii) On receiving the encrypted key-word, the cloud server will use the characteristic of relevance rating calculation to discover the top-okay applicable documents and dispatched again to the information user in which the top-okay is configured through the customers.

iv) The records customer decrypts the documents and recovers the proper records. for that reason, the blessings of TEES are without problem placed, and we complicated and quantify them.

VI. CONCLUSION

This paper is the examine of looking over encrypted records with visitors and energy performance over cellcloud storage. The proposed device deal with the single key-word seek the usage of OPE set of rules and TF-IDF desk. It's far more efficient in comparison to the traditional machine. The fundamental security demanding situations of mobile cloud garage together with statistic statistics leak, key-word documents association leak and at ease statistics acquisition arehandled by means of this machine.The proposed device only handles the unmarried keyword search. to improve the accuracy of the resultmulti-keyword seek should put into effect. The multi-keyword seek improves accuracy of result and can lessenthe site visitors by using decreasing top-k relevant documents.The contemporary OPE

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

algorithm is quite simple and it does no longer assist the multi-key-word seek. Thereforemulti-keyword seek the usage of a effective algorithm with performance can be imposing as future work.

REFERENCES

[1] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.
[2] 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.
[3] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 391–421.
[4] 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.
[5] 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.
[6] K. Kumar and Y. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" Computer, vol. 43, no. 4,pp. 51–56, 2010.
[7] A. Carroll and G. Heiser, "An analysis of power consumption in a smartphone," in Proceedings of the 2010 USENIX conference on USENIX annual technical conference. USENIX Association, 2010, pp. 271–284.
[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 829–837.
[9] A. Aizawa, "An information-theoretic perspective of tf-idf measures," Information Processing and Management, vol. 39, pp. 45– 65, 2003.
[10] Jian Li, Ruhui Ma, Haibing Guan, "TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud", IEEE Transactions on cloud computing.