Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.580 – 585

RESEARCH ARTICLE

TOWARDS SECURE PROCESSING PRIVATE QUERIES OVER ENCRYPTED CLOUD DATA

Sumathi Sivaraj[1], S. Yasotha[2]

[1]M.E Computer Science and Engineering

Sri Eshwar College of Engineering, Anna University, India

[2]M.E., (Ph.D.) Assistant professor,

Sri Eshwar College of Engineering, Anna University, India

[1] sumathi.maniyam@gmail.com ; [2] yasotha.vlsi@gmail.com

Abstract— Cloud Computing becomes prevailing, sensitive data area unit being progressively centralized into the cloud. For the protection of information privacy, sensitive knowledge needs to be encrypted before outsourcing, that makes effective knowledge utilization a awfully difficult task. Though ancient searchable cryptography schemes enable users to firmly search over encrypted knowledge through keywords, these techniques support solely mathematician search, while not capturing any connection of information files. This approach suffers from 2 main drawbacks once directly applied within the context of Cloud Computing. On the one hand, users, United Nations agency don't essentially have pre-knowledge of the encrypted cloud knowledge, ought to post method each retrieved move into order to search out ones most matching their interest; On the opposite hand, invariably retrieving all files containing the queried keyword any incurs gratuitous network traffic, that is completely undesirable in today's pay-as-you-use cloud paradigm. during this paper, for the primary time we have a tendency to outline and solve the matter of effective nevertheless secure graded keyword search over encrypted cloud knowledge. In our planned Model, we have a tendency to exhibit the Querying method over the cloud computing infrastructure mistreatment Secured & Encrypted knowledge access and Ranking over the results would profit the user for the convalescing Results.

Keywords— Network, keyword search, Information, encryption

I. INTRODUCTION

Cloud computing depends on sharing of resources to attain coherence and economies of scale, just like a utility (like the electricity grid) over a network. At the inspiration of cloud computing is that the broader construct of converged infrastructure and shared services. The cloud additionally focuses on increasing the effectiveness of the shared resources. Cloud resources area unit sometimes not solely shared by multiple users however are dynamically reallocated per demand. This will work for allocating resources to users.

Cloud computing, an important pattern for advanced information service, has became a necessary feasibleness for information users to source information. Controversies on privacy, however, are unendingly

bestowed as outsourcing of sensitive info together with emails, health history and private photos is explosively increasing. Reports of information loss and privacy breaches in cloud computing systems seem from time to time.

The main threat on information privacy roots within the cloud itself. once users source their non-public information onto the cloud, the cloud service suppliers area unit ready to management and monitor the info and also the communication between users and also the cloud at can, lawfully or unlawfully,. Instances like the key United States intelligence agency program, operating with AT&T and Verizon, that recorded over ten million phone calls between Americans, cause uncertainty among privacy advocates, and also the bigger powers it offers to telecommunication corporations to observe user activity. To confirm privacy, users sometimes write in code the info before outsourcing it onto cloud that brings nice challenges to effective information utilization. However, although the encrypted information utilization is feasible, users still must communicate with the cloud and permit the cloud care for the encrypted information that doubtless causes outflow of sensitive info.

Furthermore, in cloud computing, information house owners could share their outsourced information with variety of users, UN agency may need to solely retrieve the info files they're curious about. one among the foremost well-liked ways in which to try and do thus is thru keyword-based retrieval. Keyword-based retrieval may be a typical information service and wide applied in plaintext eventualities, within which users retrieve relevant files in a very file set supported keywords. However, it seems to be a troublesome task in ciphertext state of affairs thanks to restricted operations on encrypted information. Besides, so as to boost feasibleness and save on the expense within the cloud paradigm, it's most popular to induce the retrieval result with the foremost relevant files that match users' interest rather than all the files, that indicates that the files ought to be graded within the order of relevancy by users' interest and solely the files with the very best relevancy area unit sent back to users.

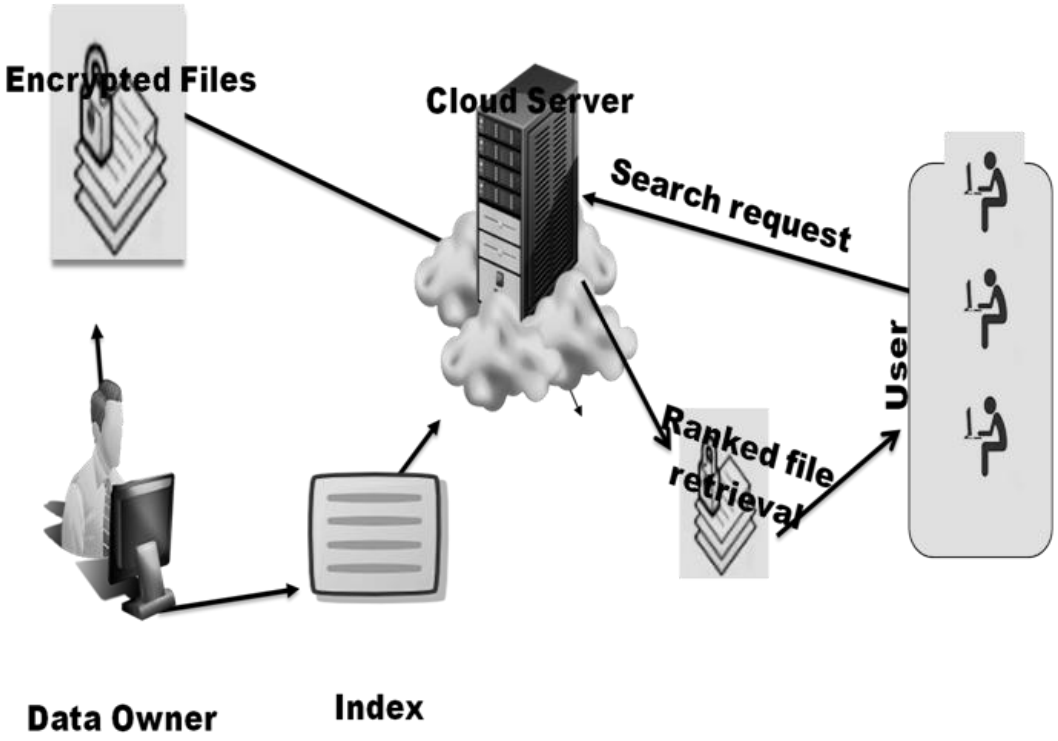

Figure 1.1 design of the search over encrypted cloud information

A series of searchable isobilateral coding schemes are planned to change search on cipher text. ancient point schemes change users to firmly retrieve the cipher text, however these schemes support solely Boolean keyword search, i.e., whether or not a keyword exists in a very file or not, while not considering the distinction of relevancy with the queried keyword of those files within the result. To boost security while not sacrificing potency, schemes bestowed in show that they support top-k single keyword retrieval below numerous eventualities. Authors of created makes an attempt to resolve the matter of top-k multi-keyword over encrypted cloud information. These schemes, however, suffer from 2 issues Boolean illustration and the way to strike a balance between security and potency. Within the former, files area unit graded solely by the amount of retrieved keywords that impairs search accuracy. Within the latter, security is implicitly compromised to exchange for potency, that is especially undesirable in security-oriented applications.

Preventing the cloud from involving in ranking and entrusting all the work to the user may be natural thanks to avoid info outflow. However, the restricted process power on the user aspect and also the high process overhead precludes info security. The problem of secure process non-public queries over encrypted cloud information therefore is: a way to create the cloud does a lot of work throughout the method of retrieval while not info outflows.

In this paper, we tend to introduce the ideas of similarity relevancy and theme lustiness to formulate the privacy issue in searchable coding schemes, so solve the insecurity drawback by proposing a two-round searchable coding (TRSE) theme. Novel technologies within the cryptography community and data retrieval community area unit utilized, together with homomorphic coding and vector area model. Within the planned theme, the bulk of computing work is completed on the cloud whereas the user takes half in ranking, that guarantees secure process non-public queries over encrypted cloud information with high security and sensible potency.

Our contributions are often summarized as follows:

- We propose the ideas of similarity relevancy and theme lustiness. we tend to therefore perform the primary plan to formulate the privacy issue in searchable coding, and that we show server aspect ranking supported order-preserving coding (OPE) inevitably violates information privacy.
- We propose a two-round searchable coding (TRSE) theme that fulfils the secure process non-public queries over encrypted cloud information. Specifically, for the primary time we tend to use relevancy score to support secure process over cloud information.
- Thorough analysis on security demonstrates the planned theme guarantees high information privacy. What is more, performance analysis and experimental results show that our theme is economical for sensible utilization.

II. OBJECTIVE OF THE WORK

The objective of this project is to inspire and solve the matter of secure knowledge retrieval over encrypted cloud knowledge. We have a tendency to outline similarity connection and theme strength. Supported order protective coding invisibly leak sensitive data, we have a tendency to devise a server-side ranking SSE theme. We have a tendency to then propose a two-round searchable coding (TRSE) theme using the absolutely homomorphism coding, that fulfils the safety needs of multi-keyword top k retrieval over the encrypted cloud knowledge. By security analysis, we have a tendency to show that the planned theme guarantees knowledge privacy.

III.EXISTING SYSTEM

3.1 Existing System Description

Cloud Computing allows cloud customers to remotely store their information into the cloud therefore on relish the on-demand top quality applications and services from a shared pool of configurable computing resources. the advantages brought by this new computing model embody however don't seem to be restricted to: relief of the burden for storage management, universal information access with freelance geographical locations, and turning away of cost on hardware, software, and personnel maintenances, etc. With the prevalence of cloud services, additional and additional sensitive data area unit being centralized into the cloud servers, like emails, personal health records, non-public videos and photos, company finance information, government documents, etc.

In past years if we would like to go looking a go in the web, we tend to continually build a question to the web server; net can retrieve the foremost variety of visited file that is named as variety of Hits. Until currently any program can retrieve the Links to the user support the frequent variety of Clicks or Hits created by the user. Therefore ranking proves is achieved mistreatment this system solely. Even some times tangential information would be hierarchical for the user that is of no use. To guard information privacy and combat uninvited accesses, sensitive information must be encrypted before outsourcing therefore on give end-to-end information confidentiality assurance within the cloud and on the far side. However, encoding makes effective information utilization a awfully difficult task provided that there may well be an oversized quantity of outsourced information files.

In cloud computing, information house owners might share their outsourced information with variety of users, United Nations agency would possibly wish to solely retrieve the information files they're curious about. One in all the foremost standard ways that to try and do therefore is thru keyword-based retrieval. Keyword-based

retrieval may be a typical information service and wide applied in plaintext situations, during which users retrieve relevant files in a very file set supported keywords. However, it seems to be a tough task in ciphertext situation attributable to restricted operations on encrypted information.

3.2 Drawbacks of Existing System

- Existing multi-keyword search support solely mathematician queries, i.e., a file either matches or doesn't match a question.

- Data storage while not cryptologic on cloud can encourage the information larceny by the malicious users.

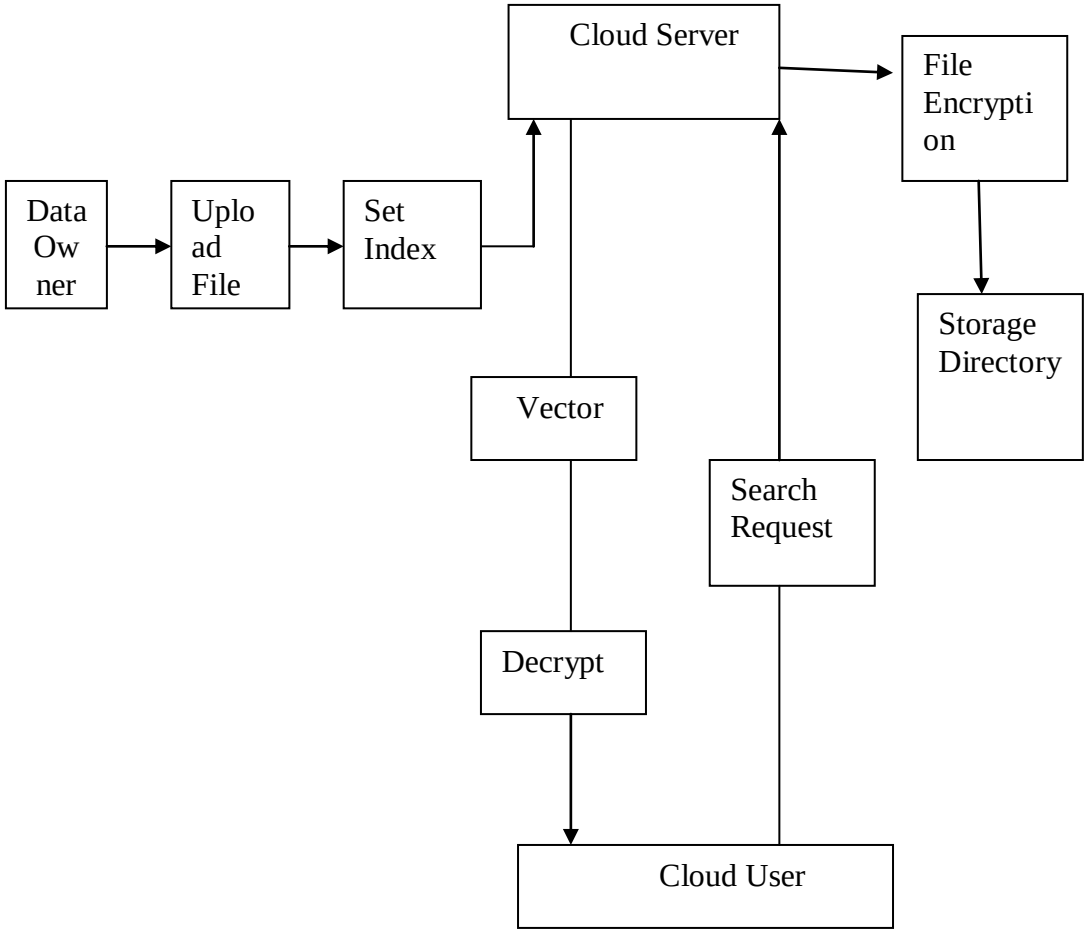

Figure 3.1 System Architecture of client server model in cloud

IV. PROPOSED SYSTEM

4.1 Proposed System Description

The cloud server hosts third-party information storage and retrieve services. Since information might contain sensitive data, the cloud servers can't be absolutely entrusted in protective information. For this reason, outsourced files should be encrypted. Any quite data escape that might have an effect on information privacy is considered unacceptable. Owner includes an assortment of n files to source onto the cloud server in encrypted type and expects the cloud server to supply keyword retrieval service to data owner himself or alternative approved users. To realize this, the information owner has to build a searchable index from a set of keywords then outsources each the encrypted index and encrypted files onto the cloud server. User is allowed to method multi-keyword retrieval over the outsourced data. The computing power on user facet is proscribed, which

suggests that operations on user facet ought to be simplified. The approved information user initially generates a question. For privacy thought, those keywords the information user has searched should be hid. Therefore the information user encrypts the question and sends it to the cloud server that returns the relevant files to the information user. Afterwards, the information user will decode and build use of the files. we tend to projected OTP (one Time Password) as our future work .This OTP accustomed see information in cloud and it is used once solely in a very time, after you search a file and have a tendency to ascertain the file the OTP can send to email and you get the OTP and apply to ascertain the file.

4.2 Benefits of Projected System

- User Ranking Guarantee why one thing is mentioned plenty, which it is not attributable to selling, or self-promotion, instead of importance.

- Proposed cloud storage systems that give confidentiality, integrity And verifiability of shopper information against an untrusted cloud supplier.

V. CONCLUSION

Solve the matter of secure information retrieval over encrypted cloud information. We tend to outline similarity connexion and theme lustiness. Supported order protective encoding invisibly leak sensitive data, we tend to devise a server-side ranking SSE theme. We tend to then propose a two-round searchable encoding (TRSE) theme using the totally homomorphic encoding, that fulfills the protection necessities of secure process non-public queries over encrypted cloud information. By security analysis, we tend to show that the planned theme guarantees information privacy. Consistent with the potency analysis of the planned theme over real dataset, in depth experimental results demonstrate that our theme ensures sensible potency.

REFERENCES

[1] Peicao, Snady Irani(1997), 'Cost-Aware WWW Proxy Caching Algorithms' in Proceedings of the USENIX Symposium on Internet Technologies and Systems.
[2] Thompson. K, Miller. G and Wilder. R(1998), 'Wilde-Area Internet Traffic Patterns and Characteristics', in Proceedings of third International Conference Web caching.
[3] Seda Cakiroglu, Erdal Arikan (2003), 'Replace Problem in Web Caching', in Proceedings of IEEE Symposium on Computers and Communications.
[4] Chrlos Maltzahn, Kathy, Richardson. J, Dirk Grunwald (1999), 'Reducing the Disk I/O of Web Proxy Server Caches', in Proceeding of the 1999 USENIX Annual Technical Conference, Monterey, California.
[5] Luigi Rizzo and Lorenzo Vicisano (2000),'Replacement Policies for a Proxy Cache', IEEE/ACM Trans Networking. Apr. 2000, pp: 158-170.
[6] Bahn. H, Noh. S and Koh. K (1999), 'Using Full Reference History for Efficient Document Replacement in net Caches', in Proceedings of the 2nd USENIX Symposium on Internet Technologies & Systems.
[7] Ying Shi, Edward Watson, and Ye-sho Chen (1997), 'Model-Driven Simulation of World-Wide-Web Cache Policies', in Proceeding of the 1997 Winter Simulation Conference, June,1997, pp: 1045-1052.
[8] Ganesh, Santhanakrishnan, Ahmed, Amer, Panos. K, Chrysanthis and Dan Li (2004), 'GDGhOST: A Goal Oriented Self Tuning Caching Algorithm', in continuing of The 19th ACM Symposium on Applied Computing.
[9] Breslau. L, Cao. L, Phillips. G and Shenker. S(1999), 'Web Caching and Zipf-like Distributions: Evidence and Implications', In continuing of Infocom 99.
[10] Ben Smith, Anurag Acharya, Tao Yang, and Huican Zhu (1999), 'Exploring Result Equivalence in Caching Dynamic Web Content' , second USENIX Symposium on Internet Technologies and Systems.

AUTHORS BIOGRAPHY

S. SUMATHI received her MCA Degree from Bharathiyar University Coimbatore, Tamilnadu, India and pursuing M.E (Computer Science and Engineering) degree from Sri Eshwar College of Engineering Coimbatore, India. Her area of interest is Network and Cloud Computing.

S.YASOTHA obtained her B.E (Computer Hardware and Software engineering) from Avinashilingam University for Women, Coimbatore (Tamilnadu, India) and received her M.E (Faculty of Information and Communication Engineering in VLSI Design) from Anna University of Technology, Coimbatore. She is pursuing Ph.D (Information and Communication Engineering in ECE Department). She is currently serving as Assistant professor of Computer Science and Engineering at Sri Eshwar college of Engineering, Coimbatore (Tamilnadu, India). Her area is Network Security and Wireless Sensor Network.

