International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey of Advance Multi-Factor Authentication and Multi-Keyword Ranked Search for Encrypted Cloud Data

Snehal Rahul Patil[1], Shiwani Sthapak[2]

[1]Research Scholar, Department of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, India

[2]Assistant Professor, Department of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, India

Abstract: ***This paper proposes a novel biometrics-based Single Sign On user authentication scheme in Telematics system, in order to enable to protect user account privacy. The focus during this work is to develop a secure and versatile multi-factor authentication to telematic environments with key management. to supply security in the use of remote crypt logical functions, we propose an authentication service embedded associate degree exceedingly in a very} key management system asatrusty third party.the most characteristics of the planned model are: flexibility, ability, safety and quality. Enabling Associate in Nursing encrypted cloud data search service is of predominant importance. Considering the massive form of data users and documents inside the cloud, it's a necessity to allow multiple keywords inside the search request and are available documents inside the order of their connectedness to those keywords. Connected works on searchable encoding specialise in single keyword search or man of science keyword search, and barely sort the search results. throughout this paper, for the 1st time, we've an inclination to stipulate and solve the tough disadvantage of privacy presering multi-keyword stratified search over encrypted cloud knowledge (MRSE).We establish a group of strict privacy wants for such a secure cloud data utilization system. Among varied multikeyword linguistics, during this paper, for the first time we've an inclination to stipulate and solve the matter of multi-keyword stratified search over encrypted cloud knowledge, and establish a variety of privacy wants. Among varied multi-keyword linguistics, we tend to elect the economical similarity live of "coordinate matching", i.e., as many matches as accomplishable, to effectively capture the connectedness of outsourced documents to the question keywords, and use "inner product similarity" to quantitatively decide such similarity live. For meeting the challenge of supporting multi-keyword linguistics while not privacy breaches, we've an inclination to propose a basic arrange of MRSE mistreatment secure complex quantity computation. Then we've an inclination to supply a pair of improved MRSE schemes to achieve varied tight privacy requirements in a pair of completely totally different threat models. Thorough analysis work privacy and efficiency guarantees of projected schemes is given, and experiments on the real-world dataset show our projected schemes introduce low overhead on every computation and communication. we tend to first propose a basic arrange for the MRSE supported secure complex quantity computation, thus provide 2 significantly improved MRSE schemes to achieve varied rigorous privacy wants in a pair of completely totally different threat models.***

Keywords: Privacy Preservation, Multikey authentication, Biometric.

1. Introduction

To protect knowledge privacy and combat uninvited accesses within the cloud and on the far side, sensitive knowledge, strong authentication methods to key management involves cryptography devices or biometrics e.g., emails, personal health records, picture albums, tax documents, financial transactions, etc., might need to be encrypted by knowledge owners before outsourcing to the business public cloud; this, however, obsoletes the standard knowledge utilization service based on plaintext keyword search. The trivial answer of downloading all the info and decrypting regionally is clearly impractical, as a result of the large quantity of information measure value in cloud scale systems. Moreover, other than eliminating the local storage management, storing knowledge into the cloud serves no purpose unless they will be simply searched and utilized. Most of the literature on the subject works with some sort of multifactor authentication and brings concepts of biometrics and cryptographic devices to increase the security. Thus, exploring privacy-preserving and effective search service over encrypted cloud knowledge is of predominant importance. Considering the potentially sizable amount of on-demand knowledge users and huge quantity of outsourced knowledge documents within the cloud, this problem is especially difficult because it is very troublesome to meet additionally the wants of performance, system usability and measurability.

Liu et al. [Liu et al., 2012] proposes a biometric-based single sign on authentication scheme for telematic systems. The proposed scheme aims to provide security for the user's account privacy replacing the traditional user and password authentication scheme. The paper works under the assumption that using a single sign on with a biometric system can guarantee the security that only the allowed user can be authenticated and after that, the user does not need to login, increasing the system usability. On the one hand, to fulfill the effective knowledge retrieval would like, the large quantity of documents demand the cloud server to perform result connexion ranking, rather than returning dedifferentiated results. Such graded search system allows knowledge users to search out the foremost relevant data quickly, rather than burdensomely sorting through each match within the content collection. graded search may elegantly eliminate unnecessary network traffic by causation back solely the foremost relevant knowledge, that is extremely fascinating within the "pay-as-youuse" cloud paradigm. For privacy protection, such ranking operation, however, mustn't leak any keyword connected information. On the opposite hand, to boost the search result accuracy likewise on enhance the user looking out expertise, it is

additionally necessary for such ranking system to support multiple keywords search, as single keyword search usually yields way too coarse results. As a typical observe indicated by today's net search engines (e.g., Google search), knowledge users might tend to provide a group of keywords rather than just one because the indicator of their search interest to retrieve the foremost relevant knowledge. And each keyword within the search request is in a position to assist slim down the search result additional. "Coordinate matching", i.e., as several matches as doable, is Associate in Nursing economical similarity measure among such multi-keyword linguistics to refine the result connexion, and has been wide utilized in the plaintext information retrieval (IR) community. However, a way to apply it within the encrypted cloud knowledge search system remains a awfully challenging task owing to inherent security and privacy obstacles, as well as varied strict needs just like the knowledge privacy, the index privacy, the keyword privacy, and many others.

In This paper, for the primary time, we have a tendency to outline and solve the problem of multi-keyword hierarchical search over encrypted cloud data (MRSE) whereas protective strict system-wise privacy in the cloud computing paradigm. Among numerous multikeyword semantics, we elect the economical similarity live of "coordinate matching", i.e., as several matches as attainable, to capture the relevancy of knowledge documents to the search query. Specifically, we have a tendency to use "inner product similarity" i.e., the number of question keywords showing in a very document, to quantitatively valuate such similarity live of that document to the search question. throughout the index construction, each document is related to a binary vector as a subindex wherever every bit represents whether or not corresponding keyword is contained within the document. The search question is also delineate as a binary vector wherever every bit suggests that whether corresponding keyword seems during this search request, so the similarity may well be precisely measured by the inner product of the question vector with the information vector. However, directly outsourcing the information vector or the question vector can violate the index privacy or the search privacy. to fulfill the challenge of supporting such multi-keyword linguistics while not privacy breaches, we have a tendency to propose a basic plan for the MRSEusing secure real computation, that is tailored from a secure k-nearest neighbor (kNN) technique, and then give 2 considerably improved MRSE schemes in a very step-bystep manner to attain numerous tight privacy needs in 2 threat models with enhanced attack capabilities. Our contributions ar summarized as follows,

1) For the first time, we explore the problem of multikeyword ranked search over encrypted cloud data, and establish a set of strict privacy requirements for such a secure cloud data utilization system.
2) We propose two MRSE schemes based on the similarity measure of "coordinate matching" while meeting different privacy requirements in two different threat models.
3) Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is given, and experiments on the real-world dataset further show the proposed schemes indeed introduce low overhead on computation and communication.

2. Literature Survey

Web users clustering is a crucial task for mining information related to users needs and preferences. Up to now, popular clustering approaches build clusters based on usage patterns derived from users' page preferences. This paper emphasizes the need to discover similarities in users' accessing behavior with respect to the time locality of their navigational acts. In this context, we present two time aware clustering approaches for tuning and binding the page and time visiting criteria. The two tracks of the proposed algorithms define clusters with users that show similar visiting behavior at the same time period, by varying the priority given to page or time visiting. The proposed algorithms are evaluated using both synthetic and real datasets and the experimentation has shown that the new clustering schemes result in enriched clusters compared to those created by the conventional non-time aware users clustering approaches behavior not only in terms of their page preferences but also of their access time. These clusters contain users exhibiting similar access

1) A break in the clouds: towards a cloud definition

L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner
Next generation computing stared with the advent of Cloud computing. In cloud computing data possessor are goaded to farm out their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. To ensure the safety of stored data, it becomes must to encrypt the data before storing. In cloud the data search arises only with the plain data. But it is essential to invoke search with the encrypted data also. The specialty of cloud data storage should allow copious keywords in a solitary query and results the data documents in the relevance order. This paper focuses on multi keyword search based on ranking over an encrypted cloud data (MRSE). The search uses the feature of similarity and inner product similarity matching. The experimental results show that the overhead in computation and communication are considerably low.

2)Cryptographic cloud storage
S. Kamara and K. Lauter
Cloud computing is becoming more interesting day by day. As the use of cloud services increases it's now important to do something for improving efficiency and security of cloud computing. Cloud storage contains huge amount of data, in such case to search that data efficiently becomes a challenging task. Also security vulnerability of such online storage systems is always non trustable. The recent researches are trying to so live this problem by the method of keyword search. But these methods solves this problem to some extend but some methods increases the computational burden on the cloud server or makes the retrieval of files the costly by means of bandwidth efficiency by sending all similar files to the requesting user. This paper discuses this problem and later gives the solution to solve this problem. To solve this problem the method of keyword search has been used. This paper tries to solve the problem of searching files through the huge amount of files securely and efficiently. The previous methods make the search non efficient by means of time and computational cost, but the

method discussed in this paper makes the searching very efficient and secure.

3) Secure indexes
E.-J. Goh,
A secure index is a data structure that allows a querier with a "trapdoor" for a word x to test
In O (1) time only if the index contains x ; The index reveals no information about its contents without valid trapdoors, and trapdoors can only be generated with a secret key. Secure indexes are a natural extension of the problem of constructing data structures with privacy guarantees such as those provided by oblivious and history independent data structures. In this paper, we formally define a secure index and formulate a security model for indexes known as semantic security against adaptive chosen keyword attack (ind-cka). We also develop an efficient ind-cka secure index construction called z-idx using pseudo-random functions and Bloom filters, and show how to use z-idx to implement searches on encrypted data. This search scheme is the most efficient encrypted data search scheme currently known; It provides O (1) search time per document, and handles compressed data, variable length words, and boolean and certain regular expression queries. The techniques developed in this paper can also be used to build encrypted searchable audit logs, private database query schemes, accumulated hashing schemes, and secure set membership tests.

4) Privacy preserving keyword searches on remote encrypted data
Y.-C. Chang and M. Mitzenmacher
Due to its low cost, robustness, flexibility and ubiquitous nature, cloud computing is changing the way entities manage their data. However, various privacy concerns arise whenever potentially sensitive data is outsourced to the cloud. This paper presents a novel approach for coping with such privacy concerns. The proposed scheme prevents the cloud server from learning any possibly sensitive plaintext in the outsourced databases. It also allows the database owner to delegate users to conducting content-level fine-grained private search and decryption. Moreover, our scheme supports private querying whereby neither the database owner nor the cloud server learns query details. Additional requirement that user's input be authorized by CA can also be supported.

5) Public key encryption with keyword search
D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano
The public key encryption with keyword search (PEKS) scheme recently proposed by Boneh, Di Crescenzo, Ostrovsky, and Persiano enables one to search encrypted keywords without compromising the security of the original data. In this paper, we address three important issues of a PEKS scheme, \refreshing keywords", \removing secure channel", and \processing multiple keywords", which have not been considered in Boneh et. al.'s paper. We argue that care must be taken when keywords are used frequently in the PEKS scheme as this situation might contradict the security of PEKS. We then point out the inefficiency of the original PEKS scheme due to the use of the secure channel. We resolve this problem by constructing an efficient PEKS scheme that removes secure channel. Finally, we propose a PEKS scheme that encrypts multiple keywords efficiently.

6)Formal proofs of cryptographic security of diffie-hellman-based protocols.
Roy, A., Datta, A., and Mitchell, J
The EAP-GPSK protocol may be a light-weight, versatile authentication pro- tocol hoping on centrosymmetric key cryptography. it's a part of AN in progress IETF process to develop authentication ways for the EAP framework. We analyze the protocol and realize 3 weaknesses: a serviceable Denial-of-Service attack, an ANomaly with the key derivation operate wont to produce a short mas- ter session key, and a ciphersuite downgrading attack. we have a tendency to propose fixes to those anomalies, and use a finite-state verification tool to look for remaining prob- lems when creating these repairs. we have a tndency to then prove the fastened version correct employing a protocol verification logic. we have a tendency to mentioned the attacks and our prompt fixes with the authors of the specification document that has afterwards been changed to include our projected changes.

3. Conclusion

In this paper, for the primary time we tend to outline and solve the problem of multi-keyword hierarchal search over encrypted cloud data, and establish a spread of privacy needs. Among various multi-keyword linguistics, we elect the economical similarity measure of "coordinate matching", i.e., as several matches as doable, to effectively capture the connectedness of outsourced documents to the question keywords, and use "inner product similarity" to quantitatively valuate such similarity live. For meeting the challenge of supporting multi-keyword linguistics without privacy breaches, we tend to propose a basic plan of MRSE using secure dot pro duct computation. Then we tend to offer 2 improved MRSE schemes to realize varied demanding privacy requirements in 2 completely different threat models. Thorough analysis investigating privacy and potency guarantees of projected schemes is given, and experiments on the real-world dataset show our projected schemes introduce low overhead on each computation and communication. In our future work, we'll explore supporting different multikeyword semantics (e.g., weighted query) over encrypted information and checking the integrity of the order within the search result.

References

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev
[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS.
[3] A. Singhal, "Modern information retrieval: A brief overview," IEEE Data Engineering Bulletin
[4] I. H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.
[6] E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, 2003, http:// eprint.iacr.org/2003 /216.
[7] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 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, 2006.
[9] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, 2004.
[10] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in Proc. of CRYPTO, 2007.
[11] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," J. Cryptol.
[12] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.
[13] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. S. III, "Public key encryption that allows pir queries," in Proc. of CRYPTO, 2007.
[14] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. of ACNS, 2004
[15] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. of ICICS, 2005.
[16] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. of TCC, 2007
[17] R. Brinkman, "Searching in encrypted data," in University of Twente PhD thesis, 2007.
[18] Y. Hwang and P. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Pairing, 2007.
[19] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. Of EUROCRYPT, 2008.
[20] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. of EUROCRYPT, 2010.
[21] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in Proc. of TCC, 2009.
[22] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.
[23] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proceedings of the 35th SIGMOD international conference on Management of data, 2009