International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-7, Issue-6S5, April 2019

Security Improvement in Open Cloud Environment Using Arithmetic Algorithm

R.Parthiban, S.G.Sandhya, U.Palani, D.Saravanan

Abstract: Cloud Based works do not provide a detailed methodological approach to elicit security and privacy requirements but methods to select cloud deployment models based on satisfaction of these requirements by Cloud Service Providers. The work introduces assurance as evidence for satisfying the security and privacy requirements in terms of completeness and reportable of security incident through audit. This allows perspective cloud users to define their assurance requirements so that appropriate cloud models can be selected for a given context.

Index Terms-Cloud deployment, security, privacy,

I.INTRODUCTION

Cloud computing is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources. Both parallel and distributed systems can be defined as a collection of processing elements that communicate and cooperate to achieve a common goal. Symmetric cryptography based schemes are clearly not suitable for this setting due to the high complexity of secret key management.

Although authorized keyword search can be realized in single-owner setting by explicitly defining a server-enforced user list that takes the responsibility to control legitimate users' search capabilities, i.e. search can only be carried out by the server with the assistance of legitimate users' complementary keys on the user list, these schemes did not realize fine-grained owner-enforced search authorization and thus are unable to provide differentiated access privileges for different users within a dataset. Asymmetric cryptography is better suited to this dynamic setting by encrypting individual contribution with different public keys.

Revised Manuscript Received on December 22, 2018.

R.Parthiban, Associate Professor, Department of CSE, IFET College of Engineering, Villupuram, parthineyveli@gmail.com
S.G.Sandhya, Associate Professor, Department of CSE, IFET College of Engineering, Villupuram, sgsandhyadhas@gmail.com
D.Saravanan, Associate Professor, Department of CSE, IFET College of Engineering, Villupuram, saranmds@gmail.com
U.Palani, Professor, Department of ECE, IFET College of Engineering, Villupuram, palani_uin@yahoo.com

II. LITERATURE SURVEY

A. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

AUTHOR - Cong Wang ; Kui Ren ; Wenjing Lou
Year 2007

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

B.Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

AUTHOR-Yao Zheng ; Kui Ren ; Wenjing LouYear 2008

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud

providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

C.Enabling Semantic Search based on Conceptual Graphs over Encrypted Outsourced Data
AUTHOR-Athanasios Vasilakos ; Ching-Nung Yang
Year 2008

Currently, searchable encryption is a hot topic in the field of cloud computing. The existing achievements are mainly focused on keyword-based search schemes, and almost all of them depend on predefined keywords extracted in the phases of index construction and query. However, keyword-based search schemes ignore the semantic representation information of users' retrieval and cannot completely match users' search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, for the first time, we define and solve the problems of semantic search based on conceptual graphs(CGs) over encrypted outsourced data in clouding computing (SSCG).We firstly employ the efficient measure of "sentence scoring" in text summarization and Tregex to extract the most important and simplified topic sentences from documents. We then convert these simplified sentences into CGs. To perform quantitative calculation of CGs, we design a new method that can map CGs to vectors. Next, we rank the returned results based on "text summarization score". Furthermore, we propose a basic idea for SSCG and give a significantly improved scheme to satisfy the security guarantee of searchable symmetric encryption (SSE). Finally, we choose a real-world dataset – ie., the CNN dataset to test our scheme. The results obtained from the experiment show the effectiveness of our proposed scheme.

D. Privacy preserving delegated word search in the cloud
AUTHOR- Kaoutar Elkhiyaoui ; Melek Önen Refik MolvaYear 2011

In this paper, we address the problem of privacy preserving delegated word search in the cloud. We consider a scenario where a data owner outsources its data to a cloud server and delegates the search capabilities to a set of third party users. In the face of semi-honest cloud servers, the data owner does not want to disclose any information about the outsourced data; yet it still wants to benefit from the highly parallel cloud environment. In addition, the data owner wants to ensure that delegating the search functionality to third parties does not allow these third parties to jeopardize the confidentiality of the outsourced data, neither does it prevent the data owner from efficiently revoking the access of these authorized parties. To these ends, we propose a word search protocol that builds upon techniques of keyed hash functions, oblivious pseudo-random functions and Cuckoo hashing to construct a searchable index for the outsourced data, and uses private information retrieval of short information to guarantee that word search queries do not reveal any information about the data to the cloud server. Moreover, we combine attribute-based encryption and oblivious pseudo-random functions to achieve an efficient revocation of authorized third parties. The proposed scheme is suitable for the cloud as it can be easily parallelized.

E. Dynamic Searchable Encryption with Multi-user Private Search for Cloud Computing
AUTHOR: Yaqiong Chen , Yousheng Zhou
YEAR 2011

Dynamic searchable encryption enables data owner to store a dynamic collection of encrypted files to the cloud server and generatesearch tokens of queries over the cloud server. Upon receiving a token, the server can perform the search on the \encrypted data while preserving privacy. Unlike many previous works that focused on a single-user scheme, we present a dynamic searchable encryption scheme with multi-user private search for cloud computing. We consider the use scenario of cloud storage services where an organization outsources its data to the cloud and authorizes a group of users to access the data. Our scheme is dependent on a red-black data structure which is highly parallelizable and dynamic, and its security is proven in the random oracle model.

III. EXISTING SYSYTEM

Cloud computing has emerged as a new enterprise IT architecture. However, privacy concern has remained a primary barrier pre-venting the adoption of cloud computing by a broader range of users/applications. When sensitive data are outsourced to the cloud, data owners naturally become concerned with the privacy of their data in the cloud and beyond. However, how the encrypted data can be effectively utilized then becomes another new challenge. Symmetric

cryptography based schemes are clearly not suitable for this setting due to the high complexity of secret key management. Although authorized keyword search can be realized in single-owner setting by explicitly defining a server-enforced user list that takes the responsibility to control legitimate users' search capabilities, i.e. search can only be carried out by the server with the assistance of legitimate users' complementary keys on the user list, these schemes did not realize fine-grained owner-enforced search authorization and thus are unable to provide differentiated access privileges for different users within a dataset. Asymmetric cryptography is better suited to this dynamic setting by encrypting individual contribution with different public keys.

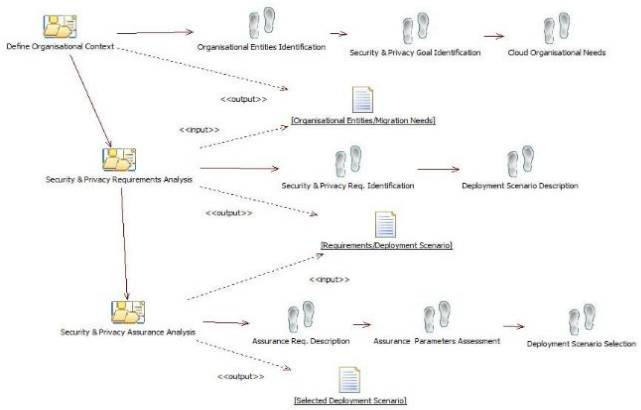
IV.PROPOSED SYSTEM

In this proposed system, we address these open issues and present an authorized keyword search scheme over encrypted cloud data with efficient user revocation in the multi-user multi-data-contributor scenario. We realize fine-grained owner-enforced search authorization by exploiting ciphertext policy attribute-based encryption (CP-ABE) technique. Specifically, the data owner encrypts the index of each file with an access policy created by him, which defines what type of users can search this index. The data user generates the trapdoor independently without relying on an always online trusted authority (TA). The cloud server (CS) can search over the encrypted indexes with the trapdoor on a user's behalf, and then returns matching result if and only if the user's attributes associated with the trapdoor satisfy the access policies embedded in the encrypted indexes. We differentiate attributes and keywords in our design. Keywords are actual content of the files while attributes refer to the properties of users.

V.ADVANTAGES OF PROPOSED SYSTEM

This system only maintains a limited number of attributes for search authorization purpose. Data owners create the index consisting of all keywords in the file but encrypt the index with an access structure only based on the attributes of authorized users, which makes more scalable and suitable for the large scale file sharing system.This scheme supports fine-grained owner-enforced search authorization at the file level with better scalability for large scale system in that the search complexity is linear to the number of attributes in the system, instead of the number of authorized users.

VI. ARCHITECTURE DIAGRAM



VII.MODULES

A module is a part of a program. Programs are composed of one or more independently developed modules that are not combined until the program is linked. A single module can contain one or several routines.

Our project modules are given below:

A. System Setup
B. New User Enrollment
C. Secure Index Generation
D. Trapdoor Generation
E. Search
F. User Revocation
G. Authenticated Search Result

A. System setup

At this initial phase, the TA defines the public parameter, and generates PK and MK. The main computation overhead is 3n exponentiations in G, one exponentiation in G1 and one pairing operation on the TA side. As the time cost for system setup is very efficient and is linear to the number of attributes in the system.

B. New user enrollment

When a new legitimate user wants to join in the system, he has to request the TA to generate the secret key SK , which needs 2n + 1 exponentiations in G. The TA also needs one exponentiation in G1 to generate a new PK component for the user. A data owner may also allow the user to access the dataset by adding him onto the corresponding user list, which incurs one exponentiation in G1. It is obvious that the time cost to enroll a new user is proportional to the number of attributes in the system.

C. Secure index generation

The size of secure index is constant if the number of attributes is pre-fixed in the system setup phase regard-less of the actual number of keywords in a file for both single keyword and conjunctive keyword search scenarios. Moreover, the data owner approximately needs (n + 1)E + E1 to generate a secure index for a file. Note that this computational burden on the data owner is a one-time cost. After all the indexes outsourced to the CS, the following index re-encryption operation is also delegated to the server. Thus, the overall efficiency for encrypting index is totally acceptable in practice.

D. Trapdoor generation

With the secret key, data user is free to produce the trapdoor of any keyword of interest, which requires about 2n + 1 group exponentiations in G. Moreover, the experimental result shows that our proposed authorized keyword search scheme enjoys very efficient trapdoor generation. In accordance with the numerical computation complexity analysis, the trapdoor generation will need more time with the increased number of attributes.

E. Search

To search over a single encrypted index, the dominant computation of ABKS-UR is n + 1 pairing operations, while APKS [21] needs n + 3 pairing operations. With the same number of system attributes, ABKS-UR is slightly faster than APKS. More-over, compared with APKS, ABKS-UR allows users to generate trapdoors independently without resorting to an always online attribute authority, and it has a broader range of applications due to the arbitrarily-structured data search capability.

F. User revocation

As the server can efficiently eliminate the revoked user's identity information from the corresponding user lists, we do not show it in Tab.1. Instead, we calculate the main computation complexity of ReKeyGen, ReEncIn-dex and ReKey. To update the system, the TA uses the algorithm ReKeyGen to produce the new version of MK′ and PK′, and the re-encryption key set rk. Depending on the number of attributes to be updated, generating rk requires minimum M to maximum Nm operations.

G. Authenticated Search Result

If the data user queries a keyword searched before, the CS will only return the search result and the user will verify them by checking the search history. Therefore no extra communication and computation overhead is introduced in this situation.

VIII.CONCLUSION

In this system, we design the first verifiable attribute-based keyword search scheme in the cloud environment, which enables scalable and fine-grained owner-enforced encrypted data search supporting multiple data owners and data users. Compared with existing public key authorized keyword search scheme, our scheme could achieve system scalability and fine-grainedness at the same time. Different from search scheme with predicate encryption, our scheme enables a flexible authorized keyword search over arbitrarily-structured data. In addition, by using proxy re-encryption and lazy re-encryption techniques, the proposed scheme is better suited to the cloud outsourcing model and enjoys efficient user revocation

REFERENCES

[1] Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud," in IEEE INFOCOM, pp. 226-234, 2014.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in Proc.of IEEE INFOCOM, pp. 1-9, 2010.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE TPDS, vol. 24, no. 1, pp. 131-143, 2013.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security, pp. 136–149, 2010.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, pp. 44-55, 2000.

[6] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure two-party computation using garbled circuits," in USENIX Security Symposium, vol. 201, no. 1, 2011.

[7] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[8] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, pp. 79-88, 2006.

[9] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of ACM CCS, pp. 965-976, 2012.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. of IEEE INFOCOM, pp. 829-837, 2011.

[11] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H.Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. of ACM ASIACCS, pp. 71-82, 2013.

[12] F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Information Security Practice and Experience, Springer, pp. 71-85, 2008.

[13] Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in Proc. of IEEE CloudCom, pp. 264-271, 2011.

[14] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. of Pairing, pp. 2-22, 2007.

[15] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. of EUROCRYPT, pp. 127-144, 1998.

[16] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. of FAST, vol. 42, pp. 29-42, 2003.

[17] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, pp. 506-522, 2004.

[18] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. of ACNS, pp. 31-45, 2004.

[19] S.Usharani, R.Ramya, "Security Based Novel Context Aware Mobile Computing Scheme Via Crowdsourcing", 2017, IJSRSET, Volume 3, Issue 2, Print ISSN: 2395-1990 ,Online ISSN :2394-4099

[20] S.Usharani, D.Saravanan,R.Parthiban "Resource Allocation through Energy In IOT Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017 IJSRCSEIT, Volume 2,Issue 3,ISSN : 2456-3307

[21] M.Sudha, D.Saravanan, S.Usharani, "Security Improvement of Dropper Elimination Scheme for IoT Based Wireless Networks", International Journal of Engineering Trends and Technology (IJETT) – Volume-45 Number3 -March 2017

[22] S.Usharani., D.Saravanan, R.Parthiban, An capable facts amalgamation come near through the guess of hazardous patients as of the original phase , International Journal of Pure and Applied Mathematics , Volume 119 No. 14 2018, 603-609

[23] R.Parthiban,D.Saravanan,S.Usharani, Worldwide center discovery using surf and sift algorithm, , International Journal of Pure and Applied Mathematics , Volume 119 No. 14 2018, 705-708.

[24] P.Manju Bala, J. Kayalvizhi, S. Usharani, D.Jayakumar, A decentralized file shareing & data transmission in peer to peer communication using edonkey protocol, International Journal of Pure and Applied Mathematics, Volume 119 No. 14 2018, 1027-1032

[25] D.Saravanan, R.Parthiban, S.Usharani, Precautions and seclusion shield in cloud computing, International Journal of Pure and Applied Mathematics, Volume 119 No. 14 2018, 849-856.

[26] M Deiva Ragavi, S Usharani, Social data analysis for predicting next event, Information Communication and Embedded Systems (ICICES), 2014 International Conference,IEEE,2014.DOI: 10.1109/ICICES.2014.7033935https: //ieeexplore.ieee.org/abstract/document/7033935/