ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Review Article*
www.ijptonline.com

A SURVEY ON EFFICIENT SECURITY ALGORITHMS IN CLOUD COMPUTING

A.Jyothsna, G.K.Sandhia
M.Tech (CSE), SRM University, Assistant Professor (OG), Department of CSE, SRM University.
Email:achunalajyothsna@gmail.com

Received on 14-11-2016 *Accepted on: 25-11-2016*

Abstract

Recently Cloud brokers are used as an additional computational layer to facilitate cloud selection and tasks of service management for cloud consumers. However, existing brokerage schemes on cloud service selection typically assume that brokers are completely allowed credit to, and do not provide any guarantee over the correctness of the service recommendations. Secure keyword search in infrastructures prevents stored documents from leaking sensitive information to unauthorized users . A shared index gives confidentiality if it is exclusively used by users authorized to search all the indexed documents. The proposed cloud-based secure data system, allows person to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of persons. Data owners can encrypt their data using **ABE Encryption Algorithm** and re-encrypt their encrypted data using **Blowfish technique** and it is combined and more secure than other Secret Sharing. To securely share the user information in cloud computing, a user divides his information M into two parts: personal information m1 that may contain the user name, social security number, telephone number, home address, etc. The official record m2 which does not contain personal information, but sensitive information's.

Keywords: Secure information retrieval, Key-Policy ABE, Blowfish.

Introduction

Keyword search is an necessary service for the automated text retrieval of diverse storage environments, such as personal content storage, online social networks, and scalable cloud facilities. As the accumulated data is becoming predominantly without a formal structure and heterogeneous, the role of text processing remains crucial in big-data analytics. Storage coherence increasingly moves sensitive data to public enterprises and makes insufficient the confidentiality achieved by storage access control alone. For instance, gathering of one's private data from seemingly unrelated sources is currently acknowleged as severe threat to the privacy of individuals. An inverted index is the

typical indexing structure of keyword search. The documents which are stored are preprocessed into a posting list per keyword (or term) with the occurrences (or postings) of the term across all the documents. Sharing of single index among multiple users offers search and storage efficiency. However, it can also leak secret information about documents with access permissions limited to a subset of the users. The problem prolongs even if a query is initially evaluated over the shared index, and the inaccessible documents are later filtered out before the final result is returned to the user.

A known secure solution serves queries from a shared index by limiting access to the postings of searchable documents, and filtering out early the postings of documents that are inaccessible to the user. In online social networks, recent research applies advanced list-processing operators and cost models to improve secure search efficiency secure keyword search in shared infrastructures prevents from leaking stored documents which have sensitive information to unauthorized users. A shared index provides confidentiality if it is exclusively used by authorized users to search all the indexed documents. We propose a cloud-based secure data system, which allows data owner to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver. To reduce the key management complexity for authority owners and data receiver .Different from previous cloud-based data system, Data owners encrypt their secret data for the data receivers using **KP-ABE Encryption scheme** and re-encrypt the encrypted data, for re-encryption **Blowfish** algorithm is proposed. Another advanced specification is, if any data receiver wants personal file to download, the data receiver will send the request to the data owner. The data owner has the Access Control. If the Owner wants to share the original file with the data receiver, he will accept receivers request and shares these keys to data receiver. After accepts request the data receiver download the secret key and use this key to download the original data. The cloud storage ensure providers that user privacy is still securely protected. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical. Attribute Based Encryption algorithm is a hierarchical structure to improve scalability and flexibility. This effectively expel the need to depend on the data storage server for preventing unauthorized data access and integrity. The proposed scheme is well organized to securely manage the data stored in the data storage servers and significantly reduces the computation time is indicated by performance measurments. To securely share the user information in cloud computing, a user divides his information M into two parts: personal information m1 that may contain the user name, social security number, telephone number, home address, etc. The official record m2 which

does not contain personal information, but sensitive informations. Then the users adopts CP-ABE scheme to encrypt the information m1 and m2 by different access policies based on the actual need. Patients can store their personal data and upload records on cloud storage. For security reasons, all data must be encrypted. It uses ABE algorithm for encryption. For Cloud storage we have configured public cloud named Dropbox cloud service. Dropbox is a personal cloud storage facility (sometimes referred to as an online backup service) that is frequently used for file sharing and cooperation. The service provides 2 gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. Dropbox is cloud storage service that enables users to store files on remote cloud servers and the ability to share files within a adjusted format. Dropbox provides an online storage solution powered by cloud computing service model of facilities as a service (IaaS). Dropbox users are provided by an online storage space hosted on Dropbox approachable anywhere via the Internet. The storage space provides storage for virtually any kind of fie type from documents, images, videos etc.

Related Work

In order to evaluate our claim of improved effectiveness, we compare the results of Security Aware Partitioning to six other partitioning methods, including process of the metadata partitioning algorithms of Smart Store and Spyglass, two recent systems doing dividing search in similar environments. [10] We propose a general set of criteria for comparing partitioning algorithms, and use them to assess the partitioning algorithms. Our results show that Security Aware Partitioning can provide excellent search action at a low computational cost to build indexes, O(n). Based on metrics such as information gain, we also conclude that costly clustering algorithms do not offer enough benefit to make them worth the additional cost in time and memory. [8] In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update load on the client will be kept minimal. In particular, we leverage the third party auditor (TPA) in many existing public auditing patterns, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the private key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's private key while doing all these burdensome tasks on behalf of the client. The client only needs to copy the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also provide the client with capability to further verify the validity of the encrypted secret keys provided by the TPA. All these noticeable features are carefully designed to make the whole auditing procedure with key exposure resistance as clear as possible for the client. We formalize the definition and the security model of this paradigm. The safety proof and the presentation simulation show that our detailed design

instantiations are secure and efficient.[5] an efficient file hierarchy attribute-based encryption scheme is put forward in cloud computing. The layered access structures are desegregated into a single access form, and then, the hierarchical files are encrypted with the integrated access structure. The cipher text modules related to attributes could be shared by the files. There by the cipher text storage and time complexity of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Exploratory simulation shows that the proposed scheme is highly well-planned in terms of encryption and decryption. With the number of the files keep on grows, the advantages of our scheme become more and more conspicuous.[7] we propose a new PEKS framework called dual-server PEKS (DS-PEKS). As another main contribution, we define a new form of the smooth projective hash functions (SPHFs) mentioned to as linear and homomorphic SPHF (LH-SPHF). We then show a general construction of secure DS-PEKS from LH-SPHF. To adorn the feasibility of our new framework, we provide an efficient methodical of the general framework from a Decision Diffie–Hellman-based LH-SPHF and show that it can attain the strong security against inside the KGA. [2] we propose a novel patient-centric framework and a set of processes for accessing and restricting of data to PHRs which are stored in semi-trusted servers. To attain fine-grained and scalable data authority for PHRs, we grip attribute based encryption (ABE) methods to encrypt each patient's PHR file using OTP (One Time Password). Unlike from previous works in secure data outsourcing, we focus on the data security outline. Our scheme also enables dynamic changes of access policies or file attributes, hold-up efficient on-demand user/attribute cancellation and break-glass access under emergency scenarios.[6] We propose an improved two-party key issuing agreement that can guarantee that neither key mastery nor cloud service provider can understand the whole secret key of a user individually. Moreover, we initiate the concept of attribute with weight, being provided to intensify the expression of attribute, which can not only expand the expression from binary to arbitrary state, but also severity the complexity of access policy. Therefore, both storage cost and encryption complication for a ciphertext are reassured. The performance examination and the security proof show that the proposed scheme is able to achieve well-organized and secure data sharing in cloud computing[1] It is common nowadays for data owners to contract out their data to the cloud. Since the cloud cannot be fully trusted, the contract out data should be encrypted. This however brings problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's contract out encrypted data? How can the data users be assured that the cloud faithfully performed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, which is known as verifiable attribute-

based keyword search (VABKS). The solution allows a data user, whose credentials pleases a data owner's access control policy, to (i) search over the data owner's contract out encrypted data, (ii) outsource the monotonous search operations to the cloud, and (iii)verify whether the cloud has faithfully performed the search operations. We formally define the security requirements of VABKS and report a construction that satisfies them. Performance assessment shows that the proposed schemes are practical and deployable. [3] We considered a new requirement of VABE with outsourced decryption: verifiability. We modified the original model of VABE with outsourced decryption proposed by Green et al. [4] to include verifiability. We also proposed a concrete VABE scheme with verifiable outsourced decryption and proved that it is secure and verifiable. Our scheme does not rely on random oracles. To evaluate the practicability of our scheme, we implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts. [9] We presented CryptDB, a system that gives a practical and strong level of confidentiality in the face of two significant warnings confronting database-backed applications: curious DBAs and arbitrary compromises of the application server and the DBMS. CryptDB meets its goals holding three ideas: running queries efficiently over encrypted data using a novel SQL-aware encryption strategy, dynamically altering the encryption level using onions of encryption to minimize the information revealed to the un-trusted DBMS server, and chaining encryption keys to user passwords in a way that allows only authenticated users to gain access to encrypted data. Our evaluation on a large trace of 126 million SQL questions from a production MySQL server shows that CryptDB can support operations over encrypted data for 99.5% of the 128,840 columns seen in the trace. The throughput sanction of CryptDB is modest, resulting in a reduction of 14.5–26% on two applications as compared to MySQL which is un-modified. Our security analysis shows that CryptDB protects most sensitive fields with highly secure encryption policies for six applications. The developer effort consists of (11–13) unique schema annotations and source code of (2-7) lines changes to express pertinent privacy policies for (22–103) sensitive fields in three multi-user web applications.

Sl No	Algorithm	Drawbacks	Description
1	Identity-Based Encryption	1. IF the key is public, someone may be able to figure out the private key. 2. For large files, strong encryption may take significant time to decrypt	ID-based encryption, or **identity-based encryption** (**IBE**), is an important primitive of ID-based cryptography. As such it is a type

		Requires a secure channel between a sender or recipient and the IBE server for transmitting the private key.	of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address).
2	AES	1. Too Simple algebraic structure. 2. Problem in sharing keys. 3. Encryption process is slow	It is a symmetric key block cipher established by the U.S. NIST in 2001. AES is based on substitution and permutation network, it is fast in both hardware and software. It has a fixed block size of 128 bits and key size of 128, 192 and256 bits. If the key size is 128 bits AES perform 10 rounds, if the key size is 192 bits it performs 12 rounds and if the key size is 256 rounds it performs 14 rounds
3	RSA	1. Public keys should/must be authenticated 2. public key encryption is slow compared to symmetric encryption 3. loss of private key may be irreparable	RSA is designed by Ron Rivest , Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system
4	Two Fish	1. A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and	Two fish is a symmetric block cipher; a single key is used for encryption and decryption. Two fish has a block size of 128 bits, and accepts a key of any length up to 256 bits. (NIST required

		rendered non-functional by an intruder. 2. High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.	the algorithm to accept 128-, 192-, and 256-bit keys.) Two fish is fast on both 32-bit and 8-bit CPUs (smart cards, embedded chips, and the like), and in hardware. And it's flexible; it can be used in network applications where keys are changed frequently and in applications where there is little or no RAM and ROM available.
5	DES	1. Two chosen input to an S-box can create the same output. 2. The purpose of initial and final permutation is not clear.	The Data Encryption Standard (DES) is a symmetric key block cipher which takes 64-bit plaintext and 56-bit key as an input and produces 64-bit cipher text as output. The DES function is made up of P and S-boxes. P-boxes transpose bits and S-boxes substitute bits to generate a cipher
6	ECC	1. ECC algorithm is more complex and more difficult to implement. 2. Main disadvantages of ECC is that it increases the size of the encrypted message	Elliptical curve cryptography is a method of encoding data files so that only specific individuals can decode them. ECC is based on the mathematics of elliptic curves and uses the location of points on an elliptic curve to encrypt and decrypt information. ECC affords efficient implementation of wireless security features.

Existing System

Secure keyword search in shared infrastructures stops stored documents from unseaworthy sensitive information to unauthorized users. A shared index provides secrecy if it is completely employed by users licensed to search all the indexed documents. We have a tendency to introduce the Lethe indexing workflow to enhance question and update

potency in secure keyword search. The Lethe workflow m clusters together documents with similar sets of licensed users, and create shared indices for configurable document subsets accessible by the constant users. We examine different datasets based on the empirical statistics of a document sharing system and various theoretical distributions. We apply Lethe to generate indexing organizations of various tradeoffs between the searches and update value. We show the lustiness of our technique by obtaining configurations of similar low prices from application of prototype-based and density-based agglomeration algorithms. With measurements over associate in nursing ASCII text file distributed search engine, we have tendency to experimentally make sure the improved search and update performance of the actual categorization configurations that we introduce.

Methodology

Secure information retrieval

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in Social network, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control. The contributions of our scheme are three aspects.

• Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.

• Secondly, we tend additionally formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) underneath the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

• Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption. It should be noticed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center.

Attribute-based encryption (ABE)

Attribute-based encryption (ABE) may be a comparitively recent approach that reconsiders the idea of public-key cryptography. In ancient public-key cryptography, a message is encrypted for a particular receiver exploiting the receiver's public-key. Identity-based cryptography associated above all and in particular identity-based encryption (IBE) modify the standard understanding of public-key cryptography by permitting the public-key to be an arbitrary

string, e.g., the email address of the receiver. ABE goes one step additional and defines the identity not atomic but as a collection of attributes, e.g., roles, and messages will be encrypted with relation to subsets of attributes (key-policy ABE - KP-ABE) or policies outlined over a collection of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that somebody ought to solely be ready to decipher a ciphertext if the person holds a key for "matching attributes" (more below) wherever user keys square measure continuously issued by some trustworthy party.

Key-Policy ABE

An important property that should be achieved by both, CP- and KP-ABE is named collusion resistance. This essentially implies that it mustn't be potential for distinct users to "pool" their secret keys along rewrite a cipher text that neither of them could rewrite on their own (which is achieved by independently randomizing users' secret keys)

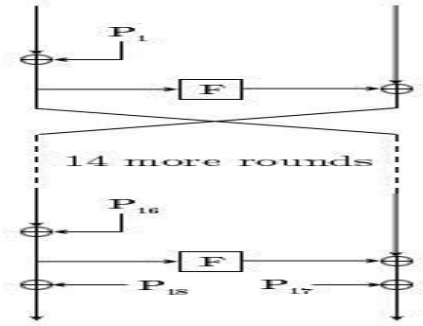
Blowfish

Blowfish was designed in 1993 by Bruce Scheier as a quick, different to existing encoding algorithms such AES, DES and three DES etc.

Blowfish may be a isosceles block encoding formula designed in thought with,

- **Fast:** It encrypts information on massive 32-bit microprocessors at a rate of twenty six clock cycles per computer memory unit.
- **Compact:** It will run in but 5K of memory.
- **Simple:** It uses addition, XOR, search table with 32-bit operands.
- **Secure:** The key length is variable, it is within the vary of 32~448 bits: default 128 bits key length.

It is appropriate for applications where the key doesn't amendment usually, like communication link or associate automatic file encryptor.



Description of Algorithm:

Blowfish trigonal block cipher algorithm program encrypts block knowledge of 64-bits at a time. It will follow the feistel network.

Key-expansion:

It will convert a key of atmost 448 bits into many sub key arrays totaling 4168 bytes. Blowfish uses sizable quantity of sub keys. These keys ar generating earlier to any secret writing or cryptography. The p-array consists of eighteen, 32-bit sub keys:

P1,P2,……,P18

Four thirty two-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,…. S1,255

S2,0, S2,1,…..S2,255

S3,0, S3,1,…..S3,255

S4,0, S4,1,.....S4,255

Conclusion

To lessen the key management complexity for data owners and data receivers. Different from previous cloud based data system, Data owners encrypt their data for using **ABE Encryption Algorithm** and re-encrypt their encrypted data using **Blowfish technique** is proposed and it is combined and more secure than other Secret Sharing algorithms and also an algorithm is proposed for data mining. Another advanced specification is, if any data receiver want personal file to download, the data receiver will send the request to the data owner. The data owner has the Access Control. If the Owner wants to share the original file with the data receiver, he shares these keys to data receiver. After accepts request the data receiver download the secret key and use this key to download the original data.

References

1. Qingji Zheng, Shouhuai Xu†,Giuseppe Ateniese . "VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data".
2. Saipavan Konda , Niranjan Reddy P "Enhanced Scalable and Secured Sharing of Personal Health Records in Cloud Computing Based on Attribute Based Encryption with Integrity Proof"
3. D.Bala Gurappa , B Dada Khalande, G. Rama Subba Reddy "KEYWORD BASED SEARCH OVER OUTSOURCED ENCRYPTED DATA USING VERIFIABLE ATTRIBUTE BASED"
4. Rui Zhang_, Rui Xue_, Ting Yuyz, and Ling Liux "PVSAE: A Public Verifiable Searchable Encryption Service Framework for Outsourced Encrypted Data"

5. Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, and Weixin Xie "An Efficient File Hierarchy Attribute-BasedEncryption Scheme in Cloud Computing"
6. Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, and Weixin Xie "Attribute-Based Data Sharing SchemeRevisited in Cloud Computing"
7. Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage Rongmao Chen, Yi Mu, *Senior Member, IEEE*, Guomin Yang, *Member, IEEE*, Fuchun Guo, and Xiaofen Wang
8. Jia Yu, Kui Ren, and Cong Wang "Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates"
9. Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan"CryptDB: Protecting Confidentiality with Encrypted Query Processing"
10. Aleatha Parker-Wood, Christina Strong, Ethan L. Miller, Darrell D.E. Long "Security Aware Partitioning for Efficient File System Search"
11. Benoit Libert , Jean-Jacques Quisquater " Efficient revocation and threshold pairing based cryptosystems" PODC '03 Boston, Massachusetts USA Copyright 2001 ACM 0-89791-88-6/97/05 ...$5.00.
12. Jae Hong Seo and Keita Emura ,"Revocable Hierarchical Identity-Based
13. Encryption: History-Free Update, Security against Insiders, and Short Cipher texts", K. Nyberg (ed.): CT-RSA 2015, LNCS 9048, pp. 106–123, 2015.
14. Jae Hong Seo and Keita Emura," Revocable Identity-Based Encryption Revisited: Security Model and Construction", January 10, 2013
15. P.-W. Chi and C.-L. Lei," Audit-free cloud Storage via deniable attribute-based encryption," IEEE Transactions on Cloud Computing, article in press (DOI: 10.1109/TCC.2015.2424882), 2015.
16. J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attributebased encryption with revocation in cloud storage," International Journal of Communication Systems, article in press (DOI: 10.1002/dac.2942), 2015.
17. H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, no. 6, pp. 487-497, 2015.
18. A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature Problems," Proc. Crypto' 86, LNCS, vol. 263, pp. 186-194, 1987.

19. K. Kurosawa and S. Heng, "From digital signature to ID-based identification/signature," Proc. PKC'04, LNCS, vol. 2947, pp 248-261, 2004.
20. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," Proc. CHES'04, LNCS, vol. 3156, pp. 357-370, 2004.
21. Y.-M. Tseng, T.-Y.Wu, and J.-D.Wu, "A pairing-based user authentication scheme for wireless clients with smart cards," Informatica, vol. 19, no. 2, pp. 285-302, 2008.
22. C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2) ," IETF, RFC 7296, 2014.
23. A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," IETF, RFC 6101, 2011.