International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 30th Nov 2019. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-11

Title **SECURED AND DUPLICATION-FREE CLOUD SERVER MAINTENANCE USING INTELLIGENT-ATTRIBUTE BASED CRYPTO-SERVICE NORMS**

Volume 08, Issue 11, Pages: 392-405.

Paper Authors

KETURU MADAN MOHAN, DR.P.PREMCHAND

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SECURED AND DUPLICATION-FREE CLOUD SERVER MAINTENANCE USING INTELLIGENT-ATTRIBUTE BASED CRYPTO-SERVICE NORMS

[1]KETURU MADAN MOHAN, [2]DR.P.PREMCHAND

[1]Research Scholar,Department of Computer Science and Engineering JNTUH, Kukatpally, 500085, Telangana State, India

[2]Professor, Department of Computer Science and Engineering University College of Engineering Osmania University, Hyderabad-500007, Telangana State, India

madan.keturu@gmail.com, prof.premchand@gmail.com

Abstract—The main objective of this cloud server maintenance system is to provide the highest safety measure to remote cloud server users with Authenticated Key Exchange Scheme [1] such as One-Time high security Passwords by using Message-Digest (MD5) algorithm as well as by the appliance of new algorithm called Intelligent-Attribute based Crypto-Service Norms (IABCSN) technique. This new methodology proves the proposed system is efficient in the sense of privacy maintenance, duplication free and enabling easy-services to all its consumers. The duplication free cloud server eliminates the content duplication, which indirectly reduces the size of server storage. The duplication elimination process allows the data owners to upload the data once into the server, the same user trying to push the same content again, the duplication-identifier does not allow to proceed further and immediately alert the user regarding this, so that the data owner can only maintain the unique data into the Cloud Server, which prevents the size of the cloud server as well as increases the speed vice-versa in data user end [1][2].

Index Terms—Cloud Computing, Privacy and Security, Data Duplication, Intelligent-Attribute based Crypto-Service Norms, IABCSN.

I. INTRODUCTION

In the technological world, each and every individual highly needs a communication port, which enables them to share the data between one and another without any range-restrictions. This provides a base for remote server maintenance scheme, Cloud a term which illustrates a server that is placed on remote environment, so that the users can use the cloud server for their communication needs in the sense of placing their data globally and provide permission to the requestors to access the data. The main roles played in the Cloud server are three members such as Data Owner, Data User and the Cloud Service Provider (CSP). In these roles data owner plays a vital lead, means the data owner only place the data into the cloud server and the regular cloud services belongs Cloud Service Providers to check the data and provide permission for the data owners to pushing that data into server and so on [3]. The major security cause occurred here, which is by means of privacy, the Cloud Service Provider is a authenticated person to provide security to cloud system as well as maintain the data owner's data, by default all the cloud server operations follow this kind approach only. However, the Cloud Service Provider is a third-person and the data owner does not forced to believe the Cloud service provider to maintain the data into server. This is the major problem we need to rectify with this work as well as the category of threat occurred in cloud server end is via

duplication of data. The data duplication problem is usually raised by data owners with their presence of knowledge or by unknowingly this may happens. The causes related to duplication of data are severe, but all the data owners are not known regarding this, the first case of affection is raised via Server Data Congestion problem, in which the data owner pushes the same data again and again means the space of the server will goes down automatically and indirectly it causes the maintenance problem as well [4][5][6]. In the side of data users, the main problem of duplication data is the lacking of required link identity, in which the data users are searching for a specific data means, the server will retrieve same data multiple times and portrait those data into user's perspective, so that the data users get confused to select the correct link to their needs. The duplication of data makes the server retrieval process too slow and the searching operations affects due to this case. The next serious issue need to be resolved is Security, the cloud server provides best services to all its consumers, it is an acceptable fact, but in case of security the following questionnaires are still need to be answered. Once the data owner pushes the data into the server, in which mean the CSP can says the data is secured without any flaws as well as the time of authentication, how the system guarantees to the data owner and data user regarding the security and access control privileges [7][8]. These two problems such as authentication security as well as data maintenance are the problematic facts need to be resolved to provide ultimate cloud security. So, that a new algorithm is required to solve these issues and provides a better security with duplication avoidance over Cloud Server, called Intelligent-Attribute based Crypto-Service Norms (IABCSN) algorithm, which efficiently reduces the security oriented issues and eliminates totally the duplication problems in the cloud server. The privacy policy of authentication is done by using multiple verifications such as while the data owner and data user registration process, the respective individuals are need to enter their identities such as name, mobile number, mail-id and so on without the option of password, so that the system first sends a high-security one time password to the given mail-id of the respective user, the user provides the correct verification code means the system allows the user to create the registration into server for further process [6][10]. In this case a question raised to everyone like how the password is given to respective user, here the proposed system follows intelligent attribute based security norm, which creates the dynamic password for the given identity and merge that identity with randomly generated key and provide a new password to user's registered e-mail-id. The mail which is sent by the system, no other person can get the password even the cloud service provider does not know about the password received by the registered user, because the server stores the encrypted password into it by means of using Message Digest (MD5) algorithm. For all the proposed system guarantees security, privacy, user-friendliness and duplication-free cloud server to maintain data properly without any flaws.

II. LITERATURE SURVEY

In the year of 2014, the authors, "S. Li and M. Xu [3]", proposed a paper titled "Attribute Attribute-Based Public Encryption with Keyword Search [3]", in that they described such as: Boneh using anonymous hierarchical identity-based encryption scheme constructed a public key searchable encryption scheme over 2004 (Public Key Encryption with Keyword Search shorthand for PEKS), which was proposed to solve the difficult task of the encrypted data to be retrieved under certain circumstances. Existing searchable encryption scheme, the mode of communication is often one-to-one; keyword cipher text can only be

queried and decrypted by a particular individual user. There are a lot of limitations in this mode of communication in the actual system. We firstly present the definition of Attribute-Based Public Encryption with Keyword Search (ATT-PEKS) and the algorithm of construction. ATT-PEKS is different from PEKS, which based on the user's property is adapt to the group's public key encryption search program, expands the information sharing, saves storage space of third-party information [2][3]. We also give the analysis of consistency and the proof of security [3].

In the year of 2014, the authors, "J. Li, Q. Wang, C. Wang, N. Cao, K . Ren, and W. Lou [6]", proposed a paper titled "Fuzzy keyword search over encrypted data in cloud computing [6]", in that they described such as Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low [6]. In this paper [6], for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search [6].

In the year of 2014, the authors, "W. Sun, S. Yu, W. Lou, Y. Hou, and H. Li [7]", proposed a paper titled "Protecting Your Right: Verifiable Attribute Attribute-Based Keyword Search with Fine Fine-Grained Owner Owner-Enforced Search Authorization in the Cloud [7]", in that they described such as: Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before-outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment [6][7]. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e., multi-user multi-contributor case. Inspired by attribute-based encryption (ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e., file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online

trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re-encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi-trusted cloud server. We formalize the security definition and prove the proposed ABKS-UR scheme selectively secure against chosen-keyword attack. To build confidence of data user in the proposed secure search system, we also design a search result verification scheme. Finally, performance evaluation shows the efficiency of our scheme.

In the year of 2015, the authors, "Q. Dong, Z. Guan, and Z. Chen [8]", proposed a paper titled "Attribute Attribute-Based Keyword Search Efficiency Enhancement via an Online/Offline Approach [8]", in that they described such as: Searchable encryption is a primitive, which not only protects data privacy of data owners but also enables data users to search over the encrypted data. Most existing searchable encryption schemes are in the single-user setting. There are only few schemes in the multiple data users setting, i.e., encrypted data sharing. Among these schemes, most of the early techniques depend on a trusted third party with interactive search protocols or need cumbersome key management. To remedy the defects, the most recent approaches borrow ideas from attribute-based encryption to enable attribute-based keyword search (ABKS). However, all these schemes incur high computational costs and are not suitable for mobile devices, such as mobile phones, with power consumption constraints. In this paper, we develop new techniques that split the computation for the keyword encryption and trapdoor/token generation into two phases: a preparation phase that does the vast majority of the work to encrypt a keyword or create a token before it knows the keyword or the attribute list/access control policy that will be used. A second phase then rapidly assembles an intermediate ciphertext or trapdoor when the specifics become known. The preparation work can be performed while the mobile device is plugged into a power source, then it can later rapidly perform keyword encryption or token generation operations on the move without significantly draining the battery. We name our scheme Online/Offline ABKS. To the best of our knowledge, this is the first work on constructing efficient multi-user searchable encryption scheme for mobile devices through moving the majority of the cost of keyword encryption and token generation into an offline phase [8].

In the year of 2016, the authors, "Y. Ye, J. Han, W. Susilo, T. H. Yuen, and J. Li [9]", proposed a paper titled "ABKS-CSC: attribute attribute-based keyword search with con stantstant-size ciphertexts [9]", in that they described such as: Attribute-based keyword search (ABKS) was proposed to enable a third party to search encrypted keywords without compromising the security of the original data. Because it can express flexible access policy, ABKS has attracted a lot of attention. Existing ABKS schemes mainly focused on the expression of access structures, while the computation cost and communication cost are linear with the number of required attributes. Therefore, existing ABKS schemes are unsuitable to the devices that have constrained space and computing power, such as smart phone and tablet. In this paper [9], an ABKS with constant-size ciphertext scheme is proposed. The proposed scheme captures the following nice features: (1) The index encryption algorithm has constant computation cost; (2) the searchable ciphertexts are constant size; (3) the trapdoors for keywords are constant size; and (4) the test algorithm has constant computation cost. To the best of our knowledge, it is the first time that an

ABKS with constant-size ciphertext scheme is proposed [9].

In the year of 2012, the authors, "Q. Chai and G. Gong [10]", proposed a paper titled "Verifiable symmetric searchable encryption for sem semi-honest-but-curious cloud servers [10]", in that they described such as Outsourcing data to cloud servers, while increasing service availability and reducing users' burden of managing data, inevitably brings in new concerns such as data privacy, since the server may be honest-but-curious. To mediate the conflicts between data usability and data privacy in such a scenario, research of searchable encryption is of increasing interest. Motivated by the fact that a cloud server, besides its curiosity, may be selfish in order to save its computation and/or download bandwidth, in this paper, the authors investigate the searchable encryption problem in the presence of a semi-honest-but-curious server, which may execute only a fraction of search operations honestly and return a fraction of search outcome honestly [10].

In the year of 2018, the authors, "H. Cui, R. H. Deng, G. Wu, and J. Lai [16]", proposed a paper titled "An Efficient and Expressive Ciphertext-Policy Attribute Attribute-Based Encryption Scheme with Partially Hidden Access Structures [16]", in that they described such as Ciphertext-policy attribute-based encryption (CP-ABE) has been regarded as one of the promising solutions to protect data security and privacy in cloud storage services. In a CP-ABE scheme, an access structure is included in the ciphertext, which, however, may leak sensitive information about the underlying plaintext and the privileged recipients in that anyone who sees the ciphertext is able to learn the attributes of the privileged recipients from the associated access structure. In order to address this issue, CP-ABE with partially hidden access structures was introduced where each attribute is divided into an attribute name and an attribute value and the attribute values of the attributes in an access structure are not given in the ciphertext [16]. Though a number of CP-ABE schemes with partially hidden access structures have been proposed, most of them only enable restricted access structures, whereas several other schemes supporting expressive access structures are computationally inefficient due to the fact that they are built in the composite-order groups. To our knowledge, there has been little attention paid to the design of expressive CP-ABE schemes with partially hidden access structures in the prime-order groups. In this paper, we revisit this problem, and present an expressive CP-ABE scheme supporting partially hidden access structures in the prime-order groups with improved efficiency [16].

In the year of 2016, the authors, "J. Li, H. Wang, and Y. Zhang [17]", proposed a paper titled "Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing [17]", in that they described such as: in ciphertext-policy attribute-based encryption (CP-ABE) scheme, a user's secret key is associated with a set of attributes, and the ciphertext is associated with an access policy. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. In the present schemes, access policy is sent to the decryptor along with the ciphertext, which means that the privacy of the encryptor is revealed. In order to solve such problem, we propose a CP-ABE scheme with hidden access policy, which is able to preserve the privacy of the encryptor and decryptor. And what's more in the present schemes, the users need to do excessive calculation for decryption to check whether their attributes match the access policy specified in the ciphertext or not, which makes the users do useless computation if the attributes don't match the hidden access policy. In order to solve efficiency issue, our scheme adds a

testing phase to avoid the unnecessary operation above before decryption. The computation cost for the testing phase is much less than the decryption computation so that the efficiency in our scheme is improved. Meanwhile, our new scheme is proved to be selectively secure against chosen-plaintext attack under DDH assumption [17].

In the year of 2018, the authors, "Y. Zhang, D. Zheng, and R. H. Deng [18]", proposed a paper titled "Security and privacy in smart health: Efficient policy policy-hiding attribute attribute-based access control [18]", in that they described such as: With the rapid development of the Internet of Things and cloud computing technologies, smart health (s-health) is expected to significantly improve the quality of health care. However, data security and user privacy concerns in s-health have not been adequately addressed. As a well-received solution to realize fine-grained access control, ciphertext-policy attribute-based encryption (CP-ABE) has the potential to ensure data security in s-health. Nevertheless, direct adoption of the traditional CP-ABE in s-health suffers two flaws. For one thing, access policies are in cleartext form and reveal sensitive health-related information in the encrypted s-health records (SHRs). For another, it usually supports small attribute universe, which places an undesirable limitation on practical deployments of CP-ABE because the size of its public parameters grows linearly with the size of the universe. To address these problems, we introduce PASH, a privacy-aware s-health access control system, in which the key ingredient is a large universe CP-ABE with access policies partially hidden. In PASH, attribute values of access policies are hidden in encrypted SHRs and only attribute names are revealed. In fact, attribute values carry much more sensitive information than generic attribute names. Particularly, PASH realizes an efficient SHR decryption test which needs a small number of bilinear pairings. The attribute universe can be exponentially large and the size of public parameters is small and constant. Our security analysis indicates that PASH is fully secure in the standard model. Performance comparisons and experimental results show that PASH is more efficient and expressive than previous schemes [18].

In the year of 2012, the authors, "Z. Wan, J. Liu, and R. H. Deng [19]", proposed a paper titled "HASBE: A Hierarchical Attribute Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing [19]", in that they described such as: Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies [19]. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational

complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments [19].

In the year of 2014, the authors, "H. Deng, Q. Wu, B. Qin, J. Domingo Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi [20]", proposed a paper titled "CiphertextCiphertext-policy hierarchical attribute attribute-based encryption with short ciphertexts [20]", in that they described such as: Attribute-based encryption (ABE) systems allow encrypting to uncertain receivers by means of an access policy specifying the attributes that the intended receivers should possess. ABE promises to deliver fine-grained access control of encrypted data. However, when data are encrypted using an ABE scheme, key management is difficult if there is a large number of users from various backgrounds. In this paper, we elaborate on ABE and propose a new versatile cryptosystem referred to as ciphertext-policy hierarchical ABE (CP-HABE). In a CP-HABE scheme, the attributes are organized in a matrix and the users having higher-level attributes can delegate their access rights to the users at a lower level. These features enable a CP-HABE system to host a large number of users from different organizations by delegating keys, e.g., enabling efficient data sharing among hierarchically organized large groups. We construct a CP-HABE scheme with short ciphertexts. The scheme is proven secure in the standard model under non-interactive assumptions [20].

In the year of 2015, the authors, "H. Li, D. Liu, Y. Dai, and T. H. Luan [21]", proposed a paper titled "Engineering searchable encryption of mobile cloud networks: when qoe meets qop [21]", in that they described such as: Mobile cloud computing can effectively address the resource limitations of mobile devices, and is therefore essential to enable extensive resource consuming mobile computing and communication applications. Of all the mobile cloud computing applications, data outsourcing, such as iCloud, is fundamental, which outsources a mobile user's data to external cloud servers and accordingly provides a scalable and “always on” approach for public data access. With the security and privacy issues related to outsourced data becoming a rising concern, encryption on outsourced data is often necessary. Although encryption increases the quality of protection (QoP) of data outsourcing, it significantly reduces data usability and thus harms the mobile user's quality of experience (QoE). How to strike a balance between QoP and QoE is therefore an important yet challenging task. In this article we focus on the fundamental problem of QoP and QoE provisioning in searchable encryption of data outsourcing. We develop a fine-grained data search scheme and discuss its implementation on encrypted mobile cloud data, which is an effective balance between QoE and QoP in mobile cloud data outsourcing [21].

In the year of 2016, the authors, "R. Chen, Y. Mu, G. Yang, F. Guo, X. Huang, X. Wang, and Y. Wang [22]", proposed a paper titled "Server-aided public key encryption with keyword search [22]", in that they described such as: Public key encryption with keyword search (PEKS) is a well-known cryptographic primitive for secure searchable data encryption in cloud storage. Unfortunately, it is inherently subject to the (inside) offline keyword guessing attack (KGA), which is against the data privacy of users. Existing countermeasures for dealing with this security issue mainly suffer from low efficiency and are impractical for real applications. In this paper, we provide a practical and applicable treatment on this security vulnerability by formalizing a new PEKS system named server-aided public key encryption with keyword search (SA-PEKS). In SA-PEKS, to

generate the keyword ciphertext/trapdoor, the user needs to query a semitrusted third-party called keyword server (KS) by running an authentication protocol, and hence, security against the offline KGA can be obtained. We then introduce a universal transformation from any PEKS scheme to a secure SA-PEKS scheme using the deterministic blind signature. To illustrate its feasibility, we present the first instantiation of SA-PEKS scheme by utilizing the Full Domain Hash RSA signature and the PEKS scheme proposed by Boneh et al. in Eurocrypt 2004. Finally, we describe how to securely implement the client-KS protocol with a rate-limiting mechanism against online KGA and evaluate the performance of our solutions in experiments [22].

In the year of 2015, the authors, "H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen [23]", proposed a paper titled "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage [23]", in that they described such as: In mobile cloud computing, a fundamental application is to outsource the mobile data to external cloud servers for scalable data storage. The outsourced data, however, need to be encrypted due to the privacy and confidentiality concerns of their owner. This results in the distinguished difficulties on the accurate search over the encrypted mobile cloud data. To tackle this issue, in this paper, we develop the searchable encryption for multi-keyword ranked search over the storage data. Specifically, by considering the large number of outsourced documents (data) in the cloud, we utilize the relevance score and k-nearest neighbor techniques to develop an efficient multi-keyword search scheme that can return the ranked search results based on the accuracy. Within this framework, we leverage an efficient index to further improve the search efficiency, and adopt the blind storage system to conceal access pattern of the search user. Security analysis demonstrates that our scheme can achieve confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user. Finally, using extensive simulations, we show that our proposal can achieve much improved efficiency in terms of search functionality and search time compared with the existing proposals [23].

In the year of 2018, the authors, "H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu [24]", proposed a paper titled "Personalized search over encrypted data with efficient and secure updates in mobile clouds [24]", in that they described such as: Mobile cloud computing has been involved as a key enabling technology to overcome the physical limitations of mobile devices toward scalable and flexible mobile services. In the mobile cloud environment, searchable encryption, which enables direct search over encrypted data, is a key technique to maintain both the privacy and usability of outsourced data in cloud. On addressing the issue, many research efforts resolve to using the searchable symmetric encryption (SSE) and searchable public-key encryption (SPE). In this paper, we improve the existing works by developing a more practical searchable encryption technique, which can support dynamic updating operations in the mobile cloud applications. Specifically, we make our efforts on taking the advantages of both the SSE and SPE techniques, and propose PSU, a Personalized Search scheme over encrypted data with efficient and secure Updates in mobile cloud. By giving thorough security analysis, we demonstrate that the PSU can achieve a high security level. Using extensive experiments in a real-world mobile environment, we show that the PUS is more efficient compared with the existing proposals [24].

In the year of 2014, the authors, "Q. Zheng, S. Xu, and G. Ateniese [25]", proposed a paper titled "Vabks: verifiable attribute based keyword search

over outsourced encrypted data [25]", in that they described such as: It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of 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 outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VA B K S and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable [25].

In the year of 2017, the authors, "J. Li, X. Lin, Y. Zhang, and J. Han [26]", proposed a paper titled "Ksf-oabe: outsourced attributebased encryption with keyword search function for cloud storage [26]", in that they described such as: Cloud computing becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing intended data users to retrieve these data stored in cloud. This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and ciphertext size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP). However, as the amount of encrypted files stored in cloud is becoming very huge, which will hinder efficient query processing. To deal with above problem, we present a new cryptographic primitive called attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function (KSF-OABE). The proposed KSF-OABE scheme is proved secure against chosen-plaintext attack (CPA). CSP performs partial decryption task delegated by data user without knowing anything about the plaintext. Moreover, the CSP can perform encrypted keyword search without knowing anything about the keywords embedded in trapdoor [26].

In the year of 2013, the authors, "Z. Liu, Z. Cao, and D. S. Wong [27]", proposed a paper titled "White-box traceable ciphertext policy attribute-based encryption supporting any monotone access structures [27]", in that they described such as: In a ciphertext-policy attribute-based encryption (CP-ABE) system, decryption keys are defined over attributes shared by multiple users. Given a decryption key, it may not be always possible to trace to the original key owner. As a decryption privilege could be possessed by multiple users who own the same set of attributes, malicious users might be tempted to leak their decryption privileges to some third parties, for financial gain as an example, without the risk of being caught. This problem severely limits the applications of CP-ABE. Several traceable CP-ABE (T-CP-ABE) systems have been proposed to address this problem, but the expressiveness of policies in those

systems is limited where only and gate with wildcard is currently supported. In this paper we propose a new T-CP-ABE system that supports policies expressed in any monotone access structures. Also, the proposed system is as efficient and secure as one of the best (non-traceable) CP-ABE systems currently available, that is, this work adds traceability to an existing expressive, efficient, and secure CP-ABE scheme without weakening its security or setting any particular trade-off on its performance [27].

In the year of 2017, the authors, "S. Qiu, J. Liu, Y. Shi, and R. Zhang [29]", proposed a paper titled "Hidden policy ciphertext policy attribute-based encryption with keyword search against keyword guessing attack [29]", in that they described such as: Attribute-based encryption with keyword search (ABKS) enables data owners to grant their search capabilities to other users by enforcing an access control policy over the outsourced encrypted data. However, existing ABKS schemes cannot guarantee the privacy of the access structures, which may contain some sensitive private information. Furthermore, resulting from the exposure of the access structures, ABKS schemes are susceptible to an off-line keyword guessing attack if the keyword space has a polynomial size. To solve these problems, we propose a novel primitive named hidden policy ciphertext-policy attribute-based encryption with keyword search (HP-CPABKS). With our primitive, the data user is unable to search on encrypted data and learn any information about the access structure if his/her attribute credentials cannot satisfy the access control policy specified by the data owner. We present a rigorous selective security analysis of the proposed HP-CPABKS scheme, which simultaneously keeps the indistinguishability of the keywords and the access structures. Finally, the performance evaluation verifies that our proposed scheme is efficient and practical [29].

In the year of 2016, the authors, "W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou [30]", proposed a paper titled "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing [30]", in that they described such as: With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with privacy preserving ranked multi-keyword search in a multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel additive order and privacy preserving function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Furthermore, PRMSM supports efficient data user revocation. Extensive experiments on real-world datasets confirm the efficacy and efficiency of PRMSM.

III. System Analysis

A. Existing System

Many cloud storage auditing schemes have been proposed up to now. These schemes consider several different aspects of cloud storage auditing

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

such as the data dynamic update the privacy protection of user's data the data sharing among multiple clients and the multi-copies of cloud data. Key-exposure resilience, as another important aspect, has been proposed recently. Indeed, the secret key might be exposed due to the weak security sense and/or the low security settings of the client. Once a malicious cloud gets the client's secret key for cloud storage auditing, it can hide the data loss incidents by forging the authenticators of fake data.

Disadvantages

- Poor Security by means of Standard Password Generation technique for Encryption and Decryption.
- Insecure Authentication Principles.
- Easy to guess passwords.

B. Proposed System

In the proposed system, we investigate how to preserve the security of cloud storage auditing scheme in any time period other than the key-exposure time period when the key exposure happens. We propose a paradigm named Intelligent-Attribute based Crypto-Service Norms (IABCSN) Scheme with intelligent server maintenance strategies to provide highest flexibility of service to all cloud users to work with the cloud environment. The proposed system is used as a practical solution for the earlier mentioned problems in the cloud server system. We design a concrete Identity Based Deduplication free resilient auditing scheme for secure cloud storage. A novel and efficient key update technique is used in the designed scheme. We formalize the definition and the security model of this new paradigm and in the security model, in this proposed scheme the most powerful adversary is considered, who can query the secret keys of the client in all except one unexposed time period. The main advantage of the proposed system is CSP can only manage the server, not interrupt with data, because system dynamically checks all without manual intervention to avoid corruptions. We formalize the definition and the security model of this new paradigm as well as in the security model, we consider the most powerful adversary who can query the secret keys of the client in all except one unexposed time period.

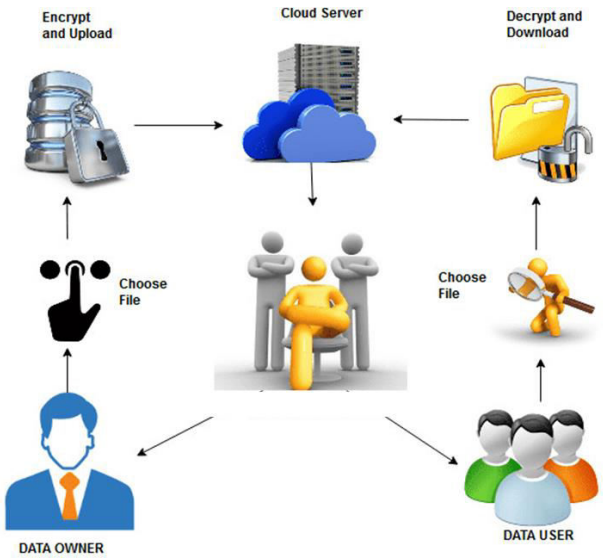

Fig.1 Proposed System Architecture Replication

Advantages

- High Security establishments by means of Identity based Proxy Encryption Methodology as well as Password Generation technique is based on IBE principles for Encryption and Decryption, so it is highly secured compare to other classical schemes.
- Secure Authentication Principles, which generates the password systematically and send to users for precedence, so it is non-guessable.

IV. CONCLUSION

When storing data on remote cloud storages, users want to be assured that their outsourced data are maintained accurately in the remote storage without being corrupted. In addition, cloud servers want to use their storage more efficiently and to

satisfy both the requirements, we proposed a scheme to achieve both secure Deduplication and integrity auditing in a cloud environment. To prevent leakage of important information about user data, the proposed scheme eliminates a data owner side duplication of encrypted data, while simultaneously supporting public auditing of encrypted data. The proposed scheme satisfied the security objectives and improved the problems of the existing schemes. In addition, it provides better efficiency than the existing schemes in the viewpoint of data user-side computational overhead and finally we designed two variations for higher security and better performance. The first variance guarantees higher security in the sense that a legitimate user can be an adversary. The second variance provides better performance from the perspective of the users (both data owners and data users), by permitting low-powered access rights to perform upload procedure very efficiently by passing their risky-operations and turn it to non-risky way.

References

[1] D.X X. Song, D. Wanger, and A. Perrig , "Practical Techniques for Searches on Encrypted Data," IEEE Symposium on Security & Privacy, Washington, DC, USA: IEEE Computer Society , May 2000, pp. 44 44-55.

[2] C. Dong, G. Russello, N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," Lecture Notes in Computer Science, Berlin, Germany: Springer, Jul. 2008, pp.127 127-143.

[3] S. Li and M. Xu, "Attribute Attribute-Based Public Encryption with Keyword Search," Chinese Journal of Computers, vol. 37, no. 5, 1018 1018-1024, Jun. 2014, doi: 10.3724/SP.J.1016.2014.01017.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, 2011, pp. 895 -93.

[5] M. Bellare , A. Boldyreva, and A. O'Neill, "Deterministic and Efficiently Searchable Encryption," the 27th annual international cryptology conference on Advances in cryptology , Berlin, Germany: Springer, Aug. 2007, pp. 535 535-552.

[6] J. Li, Q. Wang, C. Wang, N. Cao, K . Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," International Journal of Engineering Research and Applications, vol. 4, no. 7, pp. 441 441-445, May 2014, doi: 10.1109/INFCOM.2010.5462196 2010.5462196.

[7] W. Sun, S. Yu, W. Lou, Y. Hou, and H. Li, "Protecting Your Right: Verifiable Attribute Attribute-Based Keyword Search with Fine Fine-Grained Owner Owner-Enforced Search Authorization in the Cloud," IEEE INFOCOM , vol. 27, no. 4, pp. 226 226-234, Jul. 2014, doi: 10.1109/INFOCOM.2014.6847943 2014.6847943.

[8] Q. Dong, Z. Guan, and Z. Chen, "Attribute Attribute-Based Keyword Search Eff iciency Enhancement via an Online/Offline Approach," the 21th IEEE International Conference on Parallel and Distributed Systems, Dec. 2015, pp. 298 298-305.

[9] Y. Ye, J. Han, W. Susilo, T. H. Yuen, and J. Li, "ABKS ABKS-CSC: attribute attribute-based keyword search with con stantstant-size ciphertexts," Security & Communication Networks, vol. 9, no. 18, pp. 5003 5003-5015, Oct. 2016, doi: org/10.1002/sec.1671 1671. [Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for sem semi-honesthonest-butbut-curious cloud servers," IEEE International Conference on Communications, Jun. 2012, pp. 917 917-922.

[11] A. Sahai and B. Waters, "Fuzzy identity identity-based encryption," In Advances in Cryptology – EUROCRYPT, Cramer R. Eds. Berlin, Germany: Springer, 2 005, pp. 457 457-473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute Attribute-based encryption for fine fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA: ACM, 2006, pp. 89 89-98.

[13] J. Beth encourt, A. Sahai, and B. Waters, "CiphertextCiphertext-Policy Attribute Attribute-Based Encryption," in proc. IEEE Symposium on Security and Privacy Privacy, Washington, DC, USA USA: IEEE Computer Society, May 2007, pp. 321 321-334.

[14] B. Waters, "CiphertextCiphertext-Policy Attribute Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," In Public Key Cryptography – PKC, D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi Eds. Berlin, Germany: Springer, 2011, pp. 53 53-70.

[15] M. Green, S.Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," Usenix Conference on Security, USENIX Association Berkeley, CA, USA , 2011, pp. 34 34-49.

[16] H. Cui, R. H. Deng, G. Wu, and J. Lai, "An Efficient and Expressive CiphertextCiphertext-Policy Attribute Attribute-Based Encryption Scheme with Partially Hidden Access Structures." Computer Networks, vol. 133, no. 14, pp. 157 -165, May 2018, doi: org/10.1016/j.comn et.2018.01.034 2018.01.034.

[17] J. Li, H. Wang, and Y. Zhang, "CiphertextCiphertext-Policy Attribute Attribute-Based Encryption with Hidden Access Policy and Testing," Transactions on Internet & Information Systems, vol. 10, no. 7, pp. 3339 3339-3352, Jul. 2016, doi: 10.3837/tiis.2016.07.026 2016.07.026.

[18] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy policy-hiding attribute attribute-based access control," IEEE Internet of Things Journal ,vol. 3, no. 1, pp. 1 1-1, pp. 2130 2130-2145, Apr. 2018, doi: 10.1109/JIOT.2018.2825289.

[19] Z. Wan, J. Liu, and R. H. Deng , "HASBE: A Hierarchical Attribute Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security , vol. 7, no. 2, pp. 743 743-754, 2012, doi: 10.1109/TIFS.2011.2172209 2011.2172209.

[20] H. Deng, Q. Wu, B. Qin, J. Domingo Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi, "CiphertextCiphertext-policy hierarchical attribute attribute-based encryption with short ciphertexts," Information Sciences, vol. 275, no. 10, pp. 370 370-384, Aug. 2014. doi: 10.1016/j.ins.2014.01.035

[21] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.

[22] R. Chen, Y. Mu, G. Yang, F. Guo, X. Huang, X. Wang, and Y. Wang, "Server-aided public key encryption with keyword search," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2833–2842, 2016.

[23] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp. 127–138, 2015.

[24] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," IEEE Transactions on Emerging Topics in Computing, no. 1, pp. 97–109, 2018.

[25] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attributebased keyword search over outsourced encrypted data," in Proc. IEEE International Conference on Computer

Communications (INFOCOM 2014), 2014, pp. 522–530.

[26] J. Li, X. Lin, Y. Zhang, and J. Han, "Ksf-oabe: outsourced attributebased encryption with keyword search function for cloud storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715–725, 2017.

[27] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertextpolicy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 76–88, 2013.

[28] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. International Conference on Applied Cryptography and Network Security (ACNS 2008), 2008, pp. 111–129.

[29] S. Qiu, J. Liu, Y. Shi, and R. Zhang, "Hidden policy ciphertextpolicy attribute-based encryption with keyword search against keyword guessing attack," Science China Information Sciences, vol. 60, no. 5, p. 052105, 2017.

[30] W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566–1577, 2016.