ISSN : 2321-9602

Indo-American Journal of Agricultural and Veterinary Sciences




editor@iajavs.com
iajavs.editor@gmail.com

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

CIPHERTEXT CLOUD DATA KEYWORD SEARCH BASED ON VARIOUS SOURCES

[1] RANGA ISWARYA, [2] G V RAMANA

ABSTRACT:

SE, or searchable encryption, is a crucial tool for protecting the privacy and usability of cloud-based information. To provide both keyword-based retrieval and granular authorization, the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) technique employs Ciphertext-Policy Attribute-Based Encryption (CP-ABE). However, in modern CP-ABKS systems, the hyperparameter authority is responsible for the costly task of user certificate verification and distribution of secret keys. Additionally, this creates a bottleneck in performance for centralized cloud systems that are spread out. To get over these limitations and reduce the stress on devices with limited resources utilized in cloud computing, we provide a secure Multi-authority CP-ABKS (MABKS) system in this study. In addition, the MABKS system now permits attribute updates and the tracking of harmful attributes' authoritative sources. Based on the results of our in-depth security analysis, the MABKS system satisfies the criteria for selected security under both the preferred and picky models. Our trials using real-world datasets demonstrated the MABKS system's efficacy and use in practical applications.

INTRODUCTION:

Cloud-assisted outsourcing services [2, 3, 4, and 5] are becoming increasingly prevalent as a result of the convergence of cloud computing and the Internet of Things (IoT). For instance, by sending a sizeable amount of data to a cloud server managed by a third party, resource- constrained devices (such as mobile terminals orsensor nodes) can reduce the amount of data thatmust be stored locally and the amount of computation that must be performed, and they by sending a sizeable amount of data to a cloud server managed by a third party, resource- constrained devices (such as mobile terminals orsensor nodes) can reduce the amount of data thatmust be stored locally and the amount of computation that must be performed, and they

[1]PG SCHOLAR, SREE VAHINI INSTITUTE OF SCIENCE & TECHNOLOGY
[2] ASSOCIATE PROFESSOR, DEPARTMENT OF CSE IN SREE VAHINI INSTITUTE OF SCIENCE& TECHNOLOGY
TIRUVURU, KRISHNA DIST, ANDHRA PRADESH, INDIA

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

can also make it easier for other data users to share data (such as medical records in a healthcare setting). However, the outsourcing of data comes with the danger of personal information being disclosed. As a result, the encryption-before-outsourcing approach is generally used by users in order to accomplish both data security and privacy while working in an environment that is only partially trusted or is hacked. However, this makes it more difficult to retrieve or search through encrypted cloud data. As a result, searchable encryption (SE) schemes [6], [7], [8], [9], [10], and [11] have gained in popularity. SE schemes enable users to search for and selectively retrieve encrypted cloud data of interest based on keywords that the user specifies, making it possible for users to search for and retrieve cloud data of interest in a secure manner. In addition to the feature thatsafeguards users' privacy when retrievinginformation, cloud systems also need to include an essential component that allows for fine- grained access control. For example, the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) method is a workable tool that may simultaneously satisfy the goals of fine-grained data access and keyword-based ciphertext retrieval. The vast majority of currently available CP-ABKS schemes [4, 5],

[12], [13], and [14] were developed for scenarios involving a single attribute authority. In these scenarios, the single attribute authority is required to perform appropriate certificate verification [15] and secret key distribution.As a consequence of this, the single attributeauthority becomes the single-point performance bottleneck in large-scale distributed cloud systems (e.g., low resilience and inefficiency). In the event that this single attribute authority is taken down or hacked, the cloud service willalso be impacted (for example, it will be inaccessible for that period of time). For instance, data users may have to wait a considerable amount of time on the waiting list before they are able to get their respective secret keys. The performance of the secret key generation process might be adversely affected by a single-point performance bottleneck of this kind, which would also have an impact on the availability of the CP-ABKS scheme. Traditional multi-authority ABE techniques [16], [17], in which each authority controls discontinuous attribute sets in their own right, also run into this problem. For instance, in multi-authority CP-ABE schemes, the DU's attributes (such as job, skill, health, and so on) are managed by a variety of attribute authorities (such as talent market, identity verification center, hospital, and so on). These attribution authorities include talent markets, authentication centers and hospitals. The DU, however, continues to struggle with the problem described above in the event that one of the attributed authorities fails. In addition, the very act of integrating earlier attempts at multi-authority systems raises additional security difficulties. For instance, finding a malevolent authority that has issued, either purposefully or inadvertently,

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

the wrong secret keys for data users might be difficult. This could have happened for a number of reasons. With its heterogeneous architecture, the RAAC (Robust and Auditable Access Control) scheme [18] enables multiple Attribute Authorities (AAs) to separately conduct user certificate verification and generate the medium secret keys for user information on trust for the benefit of the Central Authority. This is done on behalf of the Central Authority (CA). Nevertheless, ciphertexts that are retrieved using keywords cannot be supported by this approach. This latter property is an incredibly valuable one in information retrieval systems, as it helps to alleviate the problem of systems producing a large number of search results that are unrelated to the query, which wastes both bandwidth and processing power. Furthermore, the majority of existing CP-ABKS schemes focus on defining an expressive access structure; however, the storage and computation costs associated with these schemes almost linearly increase with the number of system characteristics rather than user attributes. Hence, such systems are not ideal for wealth device distribution. In addition, malicious AAs provided by third parties may perform incorrect operations (for instance, AAs may generate the intermediate secret key for the suspected data user in a malicious or incorrect manner, as demonstrated in Section 5.2), and malicious DUs may connect private information by using private keys that are no longer valid when their attributes have really been updated in dynamic applications. Both of these issues arediscussed. A cross allusion keyword search (MABKS) scheme for data center systems is proposed in light of the above discussion, which include a single-point constraint and high huge computational requirements (which are unrealistic for resource-limited devices) that are difficult to overcome. Multi-authority architecture is shown in Fig. 1 as a contrast to single-authority infrastructure used in current designs. Data users' certificates must be validated, and intermediate secret keys must be generated for them by the MABKS system's AAs, which are then sent to the CA, which generates the final secret keys for DUs. In alarge company, for example, the only fully trusted department (that acts as CA) can generate the entire secret keys for staffs who are authorized to access critical business documents, but this bureau will be bogged down with much computational complexity when there are tremendous staffs, and even suffer from specific assessment bottleneck if this bureau is undermined or broken down. Renting numerous public servers (which operate as AAs) from other companies (such as Tencent, Amazon, Alibaba, etc.) may reduce the computational strain on the bank's totally department (see Fig. 2). While the wholeheartedly department's computers are safe from malicious attacks, the public servers may return inaccurateintermediate secret keys in order to save computation and transmission resources,Architecture with many levels of authority The holarchy in the MABKS organization allows multiple Atomic absorption spectroscopy to separately execute part of international authorization verification and medium secret keynew wave on behalf of CA, which dramatically reduces CA's computation

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

requirements. This is in contrast to the earlier single-authority CP- ABKS schemes [13], [14] (or traditional multi- authority CP-ABE schemes [16], [17], [19]), both of which were unable to avoid the hardlimit of a single feature bottleneck. [

• Search for keywords at the file level using a fine granularity. The majority of the traditional CP-ABKS systems [4, 5], and [12] have separate procedures for encrypting file keys and constructing indexes, but the MABKS system will include the secret key selected during the file key encryption phase into the indexes creation process. Therefore, the MABKS system not only enables data owners to specify the file-level fine-grained access control over encrypted cloud data, but it also makes it possible for cloud clients (such as data owners and data users) to perform keyword-based ciphertexts retrieval. This is made possible by the fact that MABKS is a cloud-based key management and key set management system.

• Tracing AAs with malicious intent. The extensive MABKS organization focuses on tracing the malignant AAs that incorrectly garner advanced secret keys for internet services in two phases (i.e., secret key ownershipaffirming and malicious AAs tracing). The classic traceable CPABE arrangements [20], [21], and [22] primarily focus on the malicious data users who may leak their secret keys to unauthorized entities.

• Attribute update. Because of the enhanced MABKS system's implementation of the attribute update, malevolent data users will not be able to access critical cloud data by abusing secret keys that are either too old or no longer in use. When compared to the attribute update mechanisms [23], [24] in prior CP-ABE schemes, which require users to update the entire ciphertext, the extended MABKS only permits data traffic and cloud servers to update a subset of the secret essential aspects and indexesconnected with the ciphertext. This is in contrast to the prior schemes, which required users to update the entire ciphertext.

RELATED WORK:

For financial and/or immediate service (for example, to further minimize the needs for data storage and computing), data owners may choose to outsource significant volumes of privacy-sensitive and security-critical data while storing their information in the cloud. Despite encryption mechanisms may safeguard the security and privacy of cloud data to some degree, one of the primary obstacles that data users must confront is retrieving encrypted cloud data. This is only one of numerous significant issues. This work specifically refers toSubstitution cipher Attribute-Based Encryption (SE) schemes and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) in order to enable keyword-based search capabilities and fine-grained access control over encrypted cloud data.

Since Boneh et al. [7] proposed the first Public-key Encryption with Keyword Search (PEKS) scheme, which enables a cloud server to identify records containing a user-specified keyword, a large number of versatile SE schemes have been

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

presented (for example, single keyword search [26], multikey word search [12], [27], ranked keyword search [28], [29], [30], and verifiable keyword search [31], [32]). These schemes have been For instance, Yang et al. [27] developed a novel conjunctive keyword search scheme equipped with a designated tester and timing enabled proxy encryption function. This scheme enables a data owner to delegate some of his or her access rights to data users who are able to carry out a search operation within a predetermined amount of time. In order to get the files that are most relevant to a search in a flexible manner, Li et al. [29] presented a ranked multi-keyword search scheme. This scheme enables the difficult logic search by making use of relevance scores and preference factors upon keywords. Taking into consideration the possibility that the semi-trusted cloud server may carry out certain search jobs and provide some inaccurate results, The first presentation of a verified conjunctive keyword search schemewas made by Sun et al. [32]. This search schemeis able to validate the validity of search results and perform file update operations in an effective and fast manner. Encryption mechanisms on their own are impractical because data owners lose direct physical control of remote cloud data when they outsource their data storage to the cloud, despite the fact that cloud data outsourcing services have appealing benefits such as elastic accessibility, strong reliability, and high availability.

CPABE can accomplish one-to-many encryption rather than one-to-one encryption, and it has been viewed as a potential technique to establishfine-grained user access. This is in contrast to typical access control systems, which can only achieve one-to-one encrypted communications. Since the first CP-ABE scheme was presented by Bethencourt et al. [33], a number of additionshave been developed that focus on all other problems. These extensions include expressive password policy [24], [34], attribute update [35],
[36], hierarchical access policies [37], hidden access legislation [38], and verifiable outsourceddecryption [39].

For instance, Balu et al. [34] introduced an expressive and verifiable CP-ABE system. They did this by exploiting the linear inter secret sharing approach, which dramatically minimizesthe costs associated with exchanging secrets. Zhang et al. [36] provided a feasible CP-ABE technique that allows for the cancellation of useraccess as well as the modification of attribute

information. Mao et al. [39] provided a generic construction of a CPA (Chosen-Plaintext Attack)-secure CP-ABE scheme with verifiable outsourced decryption. This was in response to the fact that the size of the ciphertext and the cost of decryption were growing in tandem with the complexity of the access policies. Existing CP-ABE systems have not completely resolved the issue of retrieving data based on keywords, despite the significant amount of study that has been conducted on this subject.

The Attribute-Based Encryption (ABE) [33], [40] scheme has been extended to the SE scheme so that it may be used to combat this issue.

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

In the research that has been done, an extension of this kind is also referred to as ABKS [14], [38], [41]. Existing ABKS schemes may be broadly categorized into two groups [13], which are referred to as Ciphertext-Policy ABKS (CP-ABKS) [14] and Key-Policy ABKS (KP-ABKS) [38], respectively. The CP-ABKS approach makes it possible to concurrently perform keyword-based ciphertext retrieval and fine-grained access control. For instance, Zheng et al.

[13] presented the first CP-ABKS system. This technique makes it possible for data owners to delegate search capabilities to data users by implementing access control over encrypted cloud data. [Citation needed] [Citation needed] The fact that this system only offers a single term search in circumstances with a single owner, however, has an impact on the user'soverall search experience. After that, Sun et al.

[14] proposed an approved multi-keyword search method in a demanding multi-owner situation [42] to accomplish fine-grained owner-enforced search rights. [42] This was done in order to achieve the goal.

A more secure CP-ABKS system was presented by Qi et al. [43] to ensure access policy privacy and to withstand an off-line keyword guessing attack. On the other hand, these CP-ABKS systems only enable a single attribute-authority, which may result in a single point performance bottleneck. This is due to the fact that the one and only AA in these schemes, which is also known as a CA, is required to supply both user certificate verification and secret key creation.

In addition, current multi-authority CP-ABE schemes [16, 17] that support the SE scheme cannot be immediately extended to the SE scheme in order to alleviate the problems that have been raised since each authority independently maintains distinct attribute subsets.

PROPOSED MABKS SYSTEM:

Before delving into the specifics of its design, the MABKS system's notation descriptions, which can be found in Table 3, are presented first in order to facilitate comprehension. In contrast to the traditional CP-ABKS schemes, which are able to accomplish fine-grained identity management and search term ciphertexts retrieval simultaneously by simply combining

CP-ABE and SE techniques, the MABKS system is able to gain the document fine-grained key by placing the hidden truth s Zp chosen in the file key symmetric encryption into the correlation coefficient (r building process. This allows the MABKS system to gain the ability to retrieve good cip The old single-authority CP-ABKS schemes and the cross CP-ABE schemes both, however, continue to be plagued by a chosen performance constraint. Hence

The MABKS system first uses a heterogeneous architectural feature that consists of a trusted CA and multiple AAs. It is important to keep inmind that each AA handpicked by a certain DU can perform the time-consuming authorization verification but instead generate medium secret keys for data users on behalf of CA, which eliminates the CA's computational effort

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

significantly and then avoids the single-point performance bottleneck. In addition, the encryption algorithm costs in standard CP-ABKS schemes rise with the complexity of access regulations in a linear fashion, which imposes a large processing strain on DO and DUs, respectively. After that, the updated MABKS will independently employ the online/offline ABE mechanism and the outsourced decryption technique in order to fix these two weaknesses. On the other hand, inreal-world deployments, the AAs given by third parties might potentially carry out harmful actions (such as providing data consumers with wrong intermediate encryption data).If each AA in the MABKS system has the capability to independently issue user certificate authentication and produce intermediate secret keys for DUs on behalf of the CA, then theissues of a single-point performance bottleneck and a heavy computation load on the CA may be resolved. In addition, the MABKS system features a constant-size trapdoor and ciphertexts retrieval overhead, which is relevant for deployment of resource-limited devices. Finally, the MABKS system is capable of achieving both keyword-based ciphertexts retrieval as well as quite ok access control. Authorized person DUs are able to gain and break the encryption interested search terms iff their attribute sets (respectively, trapdoors) satisfy established access structures (respectively, indexes). Despite this, the MABKS method still places a significant computational strain on DO and DUs in the encrypting and decrypting algorithms, respectively. We establish a sense of how to achieve digital encryption but also outsourced encryption process systems by utilizing the online/offline ABE [48] and outsourcing the cryptographic operations of ABE ciphertexts [49], [50], respectively. This will allow us to solve the difficult problems that have been presented. It is important to note that the only changes that have been made to the algorithms used in our MABKS system are shown in figure 7. Nevertheless, a number of other difficult problems, which will be presented in the next sections, still need to be solved.

It is necessary for the CA to create new secret keys whenever the access permissions or responsibilities of DUs are altered in reality. This ensures that DUs are unable to get unauthorized access to information by reusing secret keys that are either too old or no longer valid. In order to improve the applicability and practicability of the MABKS system in real-world circumstances, we have included support for attribute updating into the MABKS system.

The CA will first update the mastering key MSK and the strategy • PK whenever there are certain characteristics that need to be updated. After that, it will produce two transforming keys in order to update the secret key SKu,1 of DU and the indexes Ind that are stored in CSP. Finally, it adds one to the sequence number so that DUs whose characteristics match the access structure in other version numbers cannot produce valid search tokens. This prevents certain DUs from being able to generate legitimate search tokens. Take note that the MABKS system was recently installed.

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

CONCLUSION:

In this article, we offer an effective and workable MABKS system that can handle numerous authorities. This is done in order to prevent performance bottlenecks from occurring at a single location in cloud computing environments. In addition, the MABKS system that has been shown enables us to track malicious AAs (for example, in order to prevent collusion attacks) and supports attribute updating (for example, in order to prevent unauthorized access using obsolete secret keys). After that, we proved the selective security level of the system by the use of judicious and selective-attribute models while assuming decisional q-parallel BDHE and DBDH, correspondingly. We also analyzed the effectiveness of the device and proved that considerable savings in the costs of computation and storage were obtained in comparison to earlier ABKS methods. The MABKS system, on the other hand, does not handle expressive google searches like conjunctive keyword searches, fuzzy searches, subset searches, and so on. This is the system's most significant shortcoming. To ensure that the MABKS system is able to cater to a wide variety of different search requirements, the next work will center on the development of an effective and adaptable index structure.

REFERENCES

[1] Y. T. Demey and M. Wolff, "Simiss: A model-based searching strategy for inventory management systems," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 172–182, 2017.

[2] C. Huang, R. Lu, H. Zhu, J. Shao, and X. Lin, "Fssr: Fine-grained errs sharing via similarity-based recommendation in cloud-assisted ehealthcare system," in Proc. ACM on Asia Conference on Computer and

Communications Security (AsiaCCS'16), 2016, pp. 95–106.

[3] Y. Miao, J. Weng, X. Liu, K.-K. R. Choo, Z. Liu, and H. Li, "Enabling verifiable multiple keywords search over encrypted cloud data," Information Sciences, vol. 465, pp. 21–37, 2018.

[4] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2018.

[5] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attribute based keyword search over hierarchical data in cloud computing," IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2017.

[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Securityand Privacy (SP'00), 2000, pp. 44–55.

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), vol. 3027, 2004, pp. 506–522.

[8] 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, vol. 6, no. 1, pp. 97–109, 2018.J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 789–802, 2019.

[9] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Lattice-based proxy-oriented identity-based encryption with keywordsearch for cloud storage," Information Sciences, vol. PP, pp. 1–15, 2019.

[10] J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, and W. Lou, "Searchable symmetric encryption with forward search privacy," IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–15, 2019.

[11] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, "Practical attribute based multi-keyword search scheme in mobile crowdsourcing," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3008–3018, 2018.

[12] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute based keyword search over outsourced encrypted data," in Proc. IEEE Conference on Computer Communications (INFOCOM'14), 2014, pp. 522–530.

[13] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187– 1198, 2016.

[14] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications,"IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[15] M. Chase, "Multi-authority attribute based encryption," in Proc. IACR Theory of Cryptography Conference (TCC'07), 2007, pp. 515– 534.

[16] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 7, pp. 1735–1744, 2014.

[17] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "Raac: Robust andauditable access control with multiple attribute authorities for public cloud storage," IEEETransactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.

[18] V. K. A. Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," Journal of Network and Computer Applications, vol. 129, pp. 25–36, 2019.

[19] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," IEEE Transactions on InformationForensics and Security, vol. 10, no. 6, pp. 1274–

1288, 2015.

Indo-American Journal of Agricultural and Veterinary Sciences
ISSN 2321–9602 www.iajavs.com

[20] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient traceable authorization search system for secure cloud storage," IEEE Transactions on Cloud Computing, vol. PP, pp. 1–14, 2018.

[21] J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable cp-abe for cloud storage service: how to catch people leaking their access credentials effectively," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 883–897, 2018.

[22] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[23] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, 2017.

[24] Q. Xu, C. Tan, W. Zhu, Y. Xiao, Z. Fan, and F. Cheng, "Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing," 019.

[25] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vol. 403, pp. 1–14, 2017.

[26] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 746–759, 2016.

[27] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2014.

[28] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[29] 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.