MULTI-AUTHORITY ATTRIBUTE-BASED KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA

A. Bharathi[1], Sk. Karimulla[2]

[1]Assistant Professor, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

ABSTRACT

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.

I. INTRODUCTION

With the convergence of cloud computing and Internet of Things (IoT), cloud assisted outsourcing services are becoming more commonplace. For example, outsourcing significant volume of data to a third-party cloud server, resource-limited devices (e.g., mobile terminals, sensor nodes) can minimize local data storage and computation requirements and facilitate the sharing of data (e.g., health records in a healthcare con- text) with other data users. However, privacy leakage is an inherent risk in data outsourcing. Hence, one typically deploys the encryption-before-outsourcing mechanism to achieve both data security and privacy in the semi-

trusted or compromised cloud environment. This, however, restricts retrieval/searching over encrypted cloud data. Hence, the searchable encryption (SE) schemes have gained in popularity, since SE schemes allow one to securely search and selectively retrieve encrypted cloud data of interest based on user-specified keywords.

Apart from the privacy-preserving information retrieval functionality, the fine-grained access control is also an essential functionality in cloud systems.Ciphertext-PolicyAttribute-Based Keyword Search (CP-ABKS) scheme, for example, is a viable tool to achieve fine-grained access control and keyword-based ciphertexts retrieval simultaneously. Most existing CP-ABKS schemes [4], [5], [12], [13], [14] are designed for single attribute authority scenarios, where the single attribute authority needs to perform timeconsuming user certificate verification [15] and secret key distribution. This also results in the single attribute authority being the single-point performance bottleneck (e.g., poor robustness and inefficiency) in large-scale distributed cloud systems. Should this single attribute authority be compromised or offline, then the cloud service will also be affected (e.g., being unavailable during that period). For example, data users may be stuck in the waiting queue for a long time before obtaining their corresponding secret keys. Such a single- point performance bottleneck can potentially degrade secret key generation performance, and affect CP-ABKS scheme availability. Traditional multi-authority ABE schemes in which each authority separately manages disjointattribute sets also incur the same issue. For example, in multi-authority CP-ABE schemes, the DU's attributes (i.e., job, skill, health, etc.) are managed by various attribute authorities (i.e., talent market, authentication center, hospital, etc.). However, the DU still suffers from the above issue if one of the attribute authorities breaks down. Furthermore, simply combining previous multi-authority schemes also poses security concerns. For example, tracing a malicious authority that has issued, intentionally or unintentionally, incorrect secret keys for data users can be challenging.

The RAAC (Robust and Auditable Access Control) scheme [18] with heterogeneous architecture allows multiple Attribute Authorities (AAs) to independently conduct user certificate verification and generate the intermediate secret keys for data users on behalf of the Central Author- ity (CA). However, this scheme cannot support keyword- based ciphertexts retrieval. The latter is an extremely useful feature in information retrieval systems, to mitigate the issue of systems returning many irrelevant search results and resulting in bandwidth and computation resource wastage. Besides, most of existing CP-ABKS schemes focus on specifying expressive access structure, but the storage and computation costs in

these schemes almost linearly increase with the number of system attributes rather than user attributes. Hence, such schemes are not suitable for resource-limited device deployments. Furthermore, the malicious AAs provided by third-parties may conduct incorrect operations (e.g., AAs may maliciously or incorrectly generate the intermediate secret key for the suspected data user, as shown in Section 5.2), and malicious DUs may access sensitive information by using outdated secret keys when their attributes have been updated in dynamic applications.

II. LITERATURE SURVEY

In cloud storage systems, data owners may outsource a large volume of security-critical and privacy-sensitive data for economical and/or operational reasons (e.g., to further reduce data storage and computation requirements). Although encryption mechanism can protect cloud data security and privacy to some extent, the encrypted cloud data retrieval becomes one of several key challenges faced by data users. To provide keyword-based information retrieval and fine-grained access control over encrypted cloud data, this paper particularly relates to CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and SE schemes.

Since Boneh et al. [7] put forth the first Public-key encryption with Keyword Search (PEKS) scheme, which enables cloud server to identify records containing user- specified keyword, a large number of versatile SE schemes have been presented (e.g., single keyword search [26], multi-keyword search [12], [27], ranked keyword search [28], [29],

[30], verifiable keyword search [31], [32]). For example, Yang et al. [27] formed a novel conjunctive keyword search scheme with designated tester and timing enabled proxy re-encryption function, which allows a data owner to delegate his/her partial access rights to data users who are able to execute search operation in a limited period. To retrieve the most related files flexibly, Li et al. [29] gave a ranked multi-keyword search scheme by using the relevance scores and preference factors upon keywords, which supports the complicated logic search. Considering that the semi-trusted cloud server may execute a fraction of search tasks and output some false results, Sun et al. [32] first presented a verifiable conjunctive keyword search scheme, which can efficiently check the authenticity of search results and con- duct file update operations. Despite attractive advantages (e.g., elastic accessibility, strong reliability, high availability) in cloud data outsourcing services, encryption mechanism on its own is not practical since data owners lose the direct physical control of remote cloud data.

Compared with traditional access control solutions, CP- ABE can achieve one-to-many encryption rather than one- to-one and has been regarded as a promising way to achieve fine-grained access control. Since Bethencourt et al. [33] presented the first CP-ABE scheme, which avoids storing the entire user-list and verifies user access permissions, there has been a number of extensions focusing on other problems, such as expressive access policies [24], [34], attribute update [35], [36], hierarchical access policies [37], hidden access policy [38] and verifiable outsourced decryption [39]. For instance, Balu et al. [34] proposed an expressive and provable CP-ABE scheme by leveraging the linear inter secret sharing technique, which significantly reduces the secret sharing costs. Zhang et al. [36] proposed a practical CP-ABE scheme, which offers user revocation and attribute update. As the ciphertext size and decryption cost grow with the complexities of access policies, Mao et al. [39] gave the generic construction of CPA (Chosen-Plaintext Attack)-secure CP-ABE scheme with verifiable outsourced decryption. Despite the number of research efforts on this topic, existing CP-ABE schemes have not entirely solved the problem of keyword-based data retrieval.

To tackle this problem, Attribute-Based Encryption (ABE) [33], [40] scheme has been extended to SE scheme. Such an extension is also referred to as ABKS [14], [38],[41] in the literature. Existing ABKS schemes are broadly divided into two categories [13], namely Key-Policy ABKS (KP-ABKS) [38], [41] and Ciphertext-Policy ABKS (CP-ABKS) [14]. CP-ABKS scheme allows one to achieve keyword-based ciphertexts retrieval and fine-grained access control simultaneously. For example, Zheng et al. [13] gave the first CP-ABKS scheme, which enables data owner to delegate search capabilities to data users by enforcing access control over encrypted cloud data. However, this scheme just supports single keyword search in single-owner scenarios and hence affects user's search experience. After that, Sun et al. [14] presented an authorized multi-keyword search scheme in a challenging multi-owner scenario [42] to achieve fine-grained owner-enforced search privileges. Qiu et al. [43] gave a more secure CP-ABKS scheme to guarantee access policy privacy and resist off-line keyword guessing attack. However, these CP-ABKS schemes only support single attribute-authority, which may incur single- point performance bottleneck. This is because the single AA (also referred as CA) in these schemes must issue both user certificate verification and secret key generation. Furthermore, existing CP-ABE schemes [16], [17] supporting multi-authority cannot be directly extended to SE scheme to mitigate the discussed concerns since each authority separately keeps disjoint attribute subsets.

III. PROPOSED SYSTEM

SYSTEM & THREAT MODELS

We consider a cloud storage system in the cloud computing environment, which involves with five entities namely Central Authority (CA), multiple Attribute Authorities (AAs), Data Owner (DO), Cloud Service Provider (CSP) and Data User (DU). It is worth noticing that DUs are usually resource-limited entities (i.e., mobile devices, wearable devices, sensor nodes, etc.). However, the CA and multiple AAs have sufficient computation and storage capabilities to accomplish the assigned tasks.

In the cloud storage system, the DO collects files and generates the ciphertexts including indexes and file encryption key ciphertexts to relieve the computation and storage burden, the DO outsources ciphertexts to CSP which has capacities to issue huge amounts of data storage and search operations. Before conducting search queries, the DU must issue the secret key generation, which is cooperatively conducted by CA and his chosen AA.

Specifically, the DU first obtains his certificate by submitting his identity to CA, then sends his certificate to the selected AA. The AA needs to perform the user certificate verification and send the intermediate secret key to CA. The CA returns the final secret key to the DU. After that, the DU first generates the trapdoor according to his specified keyword, then sends the trapdoor (or search token) along with his attributes to CSP.

The CSP first checks whether both the attributes and trapdoor satisfy the access policy and indexes, respectively, then returns the relevant search results to DU if above two conditions hold. When gaining the search results, the DU needs to obtain the corresponding file decryption keys before he can decrypt these encrypted search results.

When the suspect AA mistakenly or intentionally outputs the incorrect intermediate secret key for a suspect DU, the CA can trace the malicious AA by interacting with the suspect DU. If the attributes of a certain DU have been updated, the CA will generate the transformation keys to update the DU's final secret key and indexes so that the malicious DU cannot access the sensitive information by using his old or outdated secret key. The role of each entity is presented as follows:

- Central authority. The CA can not only generate final secret keys for DUs but also trace the malicious AAs which generate incorrect intermediate secret keys for DUs in the extended MABKS system.
- Attribute authorities. Each AA, which has adequatestorage and computation capabilities, can separately perform user certificate validation according to DU's claimed attributes and generate the corresponding intermediate secret key on

behalf of the CA. Note that the goal of introducing multiple AAs is to relieve CA from burdensome tasks of certificate verification and key generation, and further reduce the possibili- ty of single-point performance bottleneck.

- Cloud service provider. The CSP which has numerousstore space and powerful computation capability can provide data storage and information retrieval services for DOs and DUs, respectively.

- Data owner. The DO collects and outsources his encrypted cloud data to CSP in order to share his data with multiple DUs, and significantly reduce local storage and computation burden.

- Data user. The DU can issue ciphertexts retrievalrequired 34Ements based on interested keywords before being verified his legitimacy by a certain AA and gaining the final secret key from CA.

Additionally, the CSP is an honest butcuriousentity which honestly abides by established protocols but may try to spy out some sensitive information. The CA, which should be real-time online to generate the final secret keys for DUs, is assumed to be fully trusted. The AAs provided by third-parties may perform maloperations incurred by carelessness or malicious behaviors. The malicious DUs may collude with each other or even compromise any AA to obtain unauthorized accesses beyond their access privileges. The DOs are fully credible.

VI. CONCLUSION

In this paper, we proposed an efficient and feasible MABKS system to support multiple authorities, in order to avoid having performance bottleneck at a single point in cloud systems. Furthermore, the presented MABKS system allows us to trace malicious AAs (e.g., to prevent collusion attacks) and support attribute update (e.g., to avoid unauthorized access using outdated secret keys). We then demonstrated the selective security level of the system in selective-matrix and selective-attribute models under decisional q-parallel BDHE and DBDH assumptions, respectively. We also e-valuated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes. However, the main flaw is that the MABKS system cannot support expressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. The future work will focus on building an efficient and flexible index construction so that the MABKS system is capable of supporting various search requests.

V. 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 ehrs sharing via similarity-based recommendation in cloud-assisted e-healthcare 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 Security and 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.

[9] 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.

[10] V. Srikanth. "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS" v srikanth | INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING, 20 MARCH. 2017. http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

[11] V. Srikanth. "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION" v srikanth | INTERNATIONAL JOURNAL OF INNOVATIVE ENGINEERING AND MANAGEMENT RESEARCH, 08 DECEMBER. 2017. https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

[12] V. Srikanth. "SECURED RANKED KEYWORD SEARCH OVER ENCRYPTED DATA ON CLOUD" v srikanth | INTERNATIONAL JOURNAL OF INNOVATIVE ENGINEERING AND MANAGEMENT RESEARCH, 08 Febraury. 2018. http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

[13] V. Srikanth. "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)" v srikanth | Journal of Emerging Technologies and Innovative Research (JETIR), 08 mAY. 2019. https://www.jetir.org/papers/JETIRDA06001.pdf

[14] V. Srikanth, et al. "Detection of Fake Currency Using Machine Learning Models." Deleted Journal, no. 41, Dec. 2023, pp. 31–38. https://doi.org/10.55529/ijrise.41.31.38.

[15] V. Srikanth, et al. "A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES." 25 Mar. 2023, pp. 300–305. http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf.

[16] V. Srikanth, "DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS." 25 Mar. 2023, pp. 201–209. http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf.

[17] V. Srikanth, "CHRONIC KIDNEY DISEASE PREDICTION USING MACHINELEARNINGALGORITHMS." 25 January. 2023, pp. 106–122. http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf.

[18] Srikanth veldandi, et al. "View of Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN". journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798.

[19] Srikanth veldandi, et al. "Improving Product Marketing by Predicting Early Reviewers on E-Commerce Websites." Deleted Journal, no. 43, Apr. 2024, pp. 17–25. https://doi.org/10.55529/ijrise.43.17.25.

[20] 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 Information Forensics and Security, vol. 10, no. 6, pp. 1274–1288, 2015.

AUTHOR'S PROFILE

A. BHARATHI iscurrently working as Assistant Professor in Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.

SK. KARIMULLA is pursuing MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.