Multi-authority Attribute based approach For manipulation of encrypted Data in cloud

Mrs.AISHWARYA G.,
Student of Gnanamani College of Technology Namakkal ,

A.SANGEETHA.,M.E., AP,
Gnanamani College of Technology Namakkal ,

Mr.K.VIJAYPRABAKARAN.,M.E,, AP
, *Gnanamani College of Technology Namakkal,*

Mr.M.S. SABARI.,M.E, AP
, Gnanamani College of Technology Namakkal,

Dr.R.Umamaheswari
Gnanamani College of Technology Namakkal,

ABSTRACT–The security concerns of cloud storage under the scenario where users encrypt-then-outsource data, share their outsourced data with other users, and the service provider can be queried for searching and retrieval of encrypted data. As main distinctive, we propose a security approach for storage, sharing and retrieval of encrypted data in the cloud fully constructed on the basis of attribute-based encryption (ABE) thus enabling access control mechanisms over both the encrypted data and also for the information retrieval task through search access control. Efforts have studied problems around this application scenario in different fronts: efficiency, flexibility, reliability, and security. Our proposed is 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. Proposed a practical CP-ABE scheme, which offers user revocation and attribute update. 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.

I INTRODUCTION

The privacy-preserving information retrieval functionality, the fine-grained access control is also an essential functionality in cloud systems. Ciphertext-Policy Attribute-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 are designed for single attribute authority scenarios, where the single attribute authority needs to perform time-consuming user certificate verification 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 singlepoint 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 disjoint attribute 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.

With the development of cloud computing, outsourcing data to cloud server attracts lots of attentions[1]. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys.

Introduce the notion of Public-key Authenticated Encryption with Keyword Search (PAEKS) to solve the problem[2], in which the data sender not only encrypts a keyword, but also authenticates it, so that a verifier would be convinced that the encrypted keyword can only be generated by the sender. We propose a concrete

and efficient construction of PAEKS, and prove its security based on simple and static assumptions in the random oracle model under the given security models.In recent years, the increasing popularity of cloud computing has led to a trend that data owners prefer to outsource their data to the clouds for the enjoyment of the on- demand storage and computing services[3]. For security and privacy concerns, fine-grained access control and secure data retrieval for the outsourced data is of critical importance.

Attribute-based keyword search (ABKS) scheme, as a cryptographic primitive which explores the notion of public key encryption with keyword search (PEKS) into the context of attribute-based encryption (ABE), can enable the data owner to flexibly share his data to a specified group of users satisfying the access policy and meanwhile, maintain the confidentiality and searchable properties of the sensitive data. However, in most of the previous ABKS schemes, the decryption service is not provided, and a fully trusted central authority is required, which is not practical in the scenario that the access policy is written over attributes or credentials issued across different trust domains and organizations. Moreover, the efficiency of storage and computation is also the bottleneck of implementation of ABKS scheme.

Using cloud computing, individuals can store their data on remote servers and allow data access to public users through the cloud servers[4]. As the outsourced data are likely to contain sensitive privacy information, they are typically encrypted before uploaded to the cloud. This, however, significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. In this paper, we address this issue by developing the fine-grained multi- keyword search schemes over encrypted cloud data.

II.EXISTING SYSTEM

To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Attribute-Based Encryption (ABE) is regarded as one of the most promising techniques. A salient feature of ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine-grained and secure access control for cloud storage systems.Although existing ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single- authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes. Despite the number of research efforts on this topic, existing ABE schemes have not entirely solved the problem of keyword- based data retrieval.

II PROPOSED SYSTEM

A Multi-authority Attribute-Based Keyword Search (MABKS) scheme for cloud systems to mitigate challenges due to single-point performance bottleneck and high storage and computation requirements (which are unrealistic for resource-limited devices). Key differences between multi-authority architecture in the MABKS system and single- authority architecture in existing schemes are presented in Fig. Specifically, each AA in the MABKS system maintains the entire attribute set and is responsible for verifying the validity of data users' certificates and generating intermediate secret keys for data users, and the CA outputs the final secret keys for DUs. For example, the only fully-trusted department (that acts as CA) in a large company can generate the whole secret keys for staffs who are authorized to access important company documents, but will be burdened with much computation overhead when there are massive staffs, and even suffer from single-point performance bottleneck if this department is compromised or breaks down.

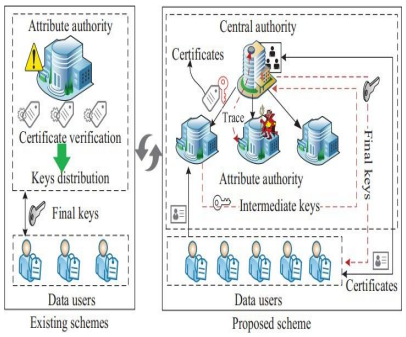

Fig 1 Proposed system

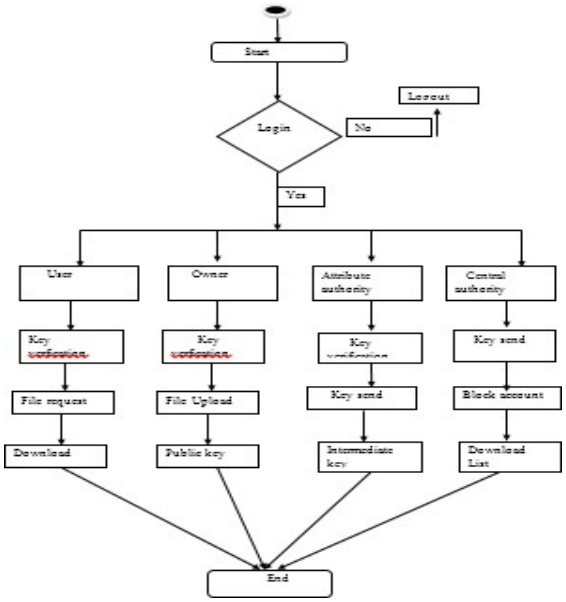

Fig 2 Flow diagram

The Java Platform

A *platform* is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware.

The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The Java platform has two components:

- The *Java Virtual Machine* (Java VM)
- The *Java Application Programming Interface* (Java API)

You've already been introduced to the Java VM. It's the base for the Java platform and is ported onto various hardware-based platforms.

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as *packages*. The next section, What Can Java Technology Do? Highlights what functionality some of the packages in the Java API provide.

The following figure depicts a program that's running on the Java platform. As the figure shows, the JavaAPI and the virtual machine insulate the program from the hardware.

VI CONCLUSION

In this project 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 also evaluated the system's performance and demonstrated that significant computation and storage cost reductions. we review the features, advantages and disadvantages of different multi- authority attribute based encryption schemes. The ultimate goal of designing a MAABE scheme is to developed a secure, robust, expressive and efficient multi-authority attribute based encryption system. Supporting client renouncement isan essential issue in the original application, and this is an impressive test the application. Blocking system is very useful for our concept to Avoid from attacker we Include blocking system.

REFERENCES

[1] A. Bagherzandi, B. Hore, and S. Mehrotra, Search over Encrypted Data. Boston, MA, USA: Springer, 2011, pp. 1088–1093.

[2] H. Pham, J. Woodworth, and M. A. Salehi, ''Survey on secure search over encrypted data on the cloud,'' Concurrency Comput. Pract. Exper., vol. 31, p. 1– 15, Apr. 2019.

[3] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[4] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[5] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[6] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[7] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.
[8] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.
[9] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[10] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749
[11] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
[12] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[13] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Areabof Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019
[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ''Searchable symmetric encryption: Improved definitions and efficient constructions,'' in Proc. 13th ACM Conf. Comput. Commun. Secur., New York, NY, USA, 2011, pp. 79–88, 2006.
[15] M. Zeng, H.-F. Qian, J. Chen, and K. Zhang, ''Forward secure public key encryption with keyword search for outsourced cloud storage,'' IEEE Trans. Cloud Comput., early access, Sep. 27, 2019, doi: 10.1109/TCC.2019.2944367.
[16] S. Kamara, C. Papamanthou, and T. Roeder, ''Cs2: A searchable cryptographic cloud storage system,'' Microsoft Res., Redmond, WA, USA, Tech. Rep. MSR-TR-2011-58, May 2011.
[17] W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, ''A privacypreserved full-text retrieval algorithm over encrypted data for cloud storage applications,'' J. Parallel Distrib. Comput., vol. 99, pp. 14–27, Jan. 2017.
[18] A. G. Kumbhare, Y. Simmhan, and V. Prasanna, ''Designing a secure storage repository for sharing scientific datasets using public clouds,'' in Proc. 2nd Int. workshop Data Intensive Comput. Clouds, 2011, pp. 31–40.
[19] Z. Yang, J. Tang, and H. Liu, ''Cloud information retrieval: Model description and scheme design,'' IEEE Access, vol. 6, pp. 15420–15430, 2018.
[20] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, ''CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme,'' IEEE Access, vol. 7, pp. 5682–5694, 2019.