Enhanced Cloud Storage Mechanism Using Security Techniques

Maheskumar.V [1],Dhaniskumar.S[2], Dharman.K [3], Karthikeyan [4]
[1, 2, 3, 4] Dept of Computer Science And Engineering
[1, 2, 3, 4] Paavai Engineering College,Namakkal

Abstract- *Cloud computing has emerging as a promising pattern for data outsourcing and high quality data services. However, concerns of sensitive information on cloud potentially cause privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, we focus on addressing data privacy issues using searchable symmetric encryption (SSE). For the first time, we formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-k multi-keyword retrieval. In TRSE, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext. As a result, information leakage can be eliminated and data security is ensured. Thorough security and performance analysis show that the proposed scheme guarantees high security and practical efficiency.*

I. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST): Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a “cloud computing” service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a “cloud computing” service. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. For that reason the Office of the Privacy Commissioner of Canada (OPC) has prepared some responses to Frequently Asked Questions (FAQs). We have also developed a Fact Sheet that provides detailed information on cloud computing and the privacy challenges it presents. Access control is essential when unauthorized users tries to access the data from the storage, so that only authorized users can access the data. It is also significant to verify that the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques. There are three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. Data should be accessed by users who have matching roles. The roles are declare by the system.

Cloud computing is emerging at the convergence of three major trends — service orientation, virtualization and standardization of computing through the Internet. Cloud computing enables users and developers to utilize services without knowledge of, expertise with, nor control over the technology infrastructure that supports them. The concept generally incorporates combinations of the following:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

Users avoid Capital Expenditure (CapEx) on hardware, software, and services when they pay a provider only for what they use. Consumption is billed on a utility (e.g. resources consumed, like electricity) or subscription (e.g. time based, like a newspaper) basis with little or no upfront cost. Cloud computing technology has been a new buzzword in the IT industry and expecting a new horizon for coming world. It is a style of computing which is having dynamically scalable virtualized resources provided as a service over the Internet. It reduces the time required to procure heavy resources and boot new server instances in minutes, allowing oneto quickly scale capacity, both up and down, as ones requirement changes.

II. IDENTIFY,RESEARCH AND COLLECT IDEA

EXISTING SYSTEM

Cloud storage service has shown its great power and wide popularity which provides fundamental support for rapid development of cloud computing. However, due to management negligence and malicious attack, there still security incidents that lead to quantities of sensitive data leakage at cloud storage layer.

DISADVANTAGES

- Very inefficient to achieve ranked search data and
- Suitably weaken the security guarantee.
- Every block is always encrypted in the same way.

PROPOSED SYSTEM

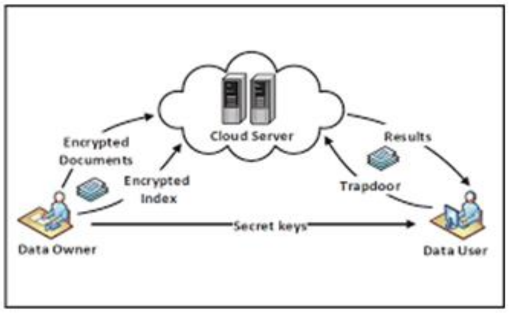
We introduce the concepts of similarity relevance and scheme robustness to formulate the privacy issue in searchable encryption schemes, and then solve the insecurity problem by proposing a two-round searchable encryption (TRSE) scheme. Novel technologies in the cryptography community and information retrieval community are employed, including homomorphic encryption and vector space model. In the proposed scheme, the majority of computing work is done on the cloud while the user takes part in ranking, which guarantees top k multi-keyword retrieval over encrypted cloud data with high security and practical efficiency.

ADVANTAGES OF THE PROPOSED SYSTEM

- It is suitable for different cloud applications and infrastructures.
- The more efficient searchable technique.
- Backup service and security.
- Data privacy and combating unsolicited accesses.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

ARCHITECTURE



Architecture diagram

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information. The output form of an information system should accomplish one or more of the following objectives.
- Convey information about past activities, current status or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

SYSTEM TESTING

TESTING TECHNIQUES

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

BLACK BOX TESTING

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. The test provides inputs and responds to outputs without considering how the software works. The coding are not tested but the forms are tested.

WHITE BOX TESTING

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It means as the coding are to be tested.

UNIT TESTING

Unit tests ensure that each unique path of a process performs accurately to the documented specifications and contains clearly defined inputs and expected results. Unit testing are tested by the each modules. First unit testing and then go to the testing.

SYSTEM IMPLEMENTATION

System design is a solution to the creation of a new system. It provides the understanding and procedural details necessary for implementing the system. The emphasis is on translating the performance requirements into the design specification. Design goes through logical and physical stages of the development. Logical design, reviews the present physical stages, makes edit security and control output specifications. The physical design maps out the physical system, plans the system implementation plan and specifies any new hardware and software.

IV. CONCLUSION

For the issue of cloud data leakage caused by management negligence and malicious attack at storage layer, we proposed CSSM, a cloud secure storage mechanism. CSSM adopted a combined approach of data dispersal and encryption technologies, which can improve the data security and pre- vent attackers from stealing user data. The experimental results show that CSSM can effectively prevent user data leakage at cloud storage layer. we introduce a novel Dynamic Searchable Symmetric Encryption (DSSE) framework called Incidence Matrix (IM)-DSSE, which achieves a high level of privacy, efficient search/update, and low client storage with actual deployments on real cloud settings.

V. FUTUREENHANCEMENT

Industrial Control Systems have migrated from being dedicated, air-gapped, centralized infrastructures and have adopted the distributed, corporate systems accessible Internet. Although the efficiency, speed, precision quality is increased, this has exposed ICS to the unsecured Internet. In this way, the proposed multi-sensor interface can achieve the compactness and the flexibility of the sensor module by utilizing two reconfigurable methods for various sensor interfaces and also by migrating most of the burdens for signal calibration and analysis to a smart phone. Thereby the sensor module itself can achieve a low-cost bill of materials (BOM) and can maximize the usage time of its internal battery by powering a minimal number of components and by optimally reconfiguring its internal operations.

REFERENCES

[1] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, ``Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," IEEE Access, vol. 8, pp. 104956104966, 2020.

[2] M. Kumar, A. Rani, and S. Srivastava, ``Image forensics based on lighting estimation," Int. J. Image Graph., vol. 19, no. 3, Jul. 2019, Art. no. 1950014.

[3] J. Li, Y. Zhang, X. Chen, and Y. Xiang, ``Secure attribute-based data sharing for resource-limited users in cloud computing," Computer Secure., vol. 72, pp. 112, Jan. 2018.

[4] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, ``Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," Inf. Sci., vol. 379, pp. 4261, Feb. 2017.

[5] The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: Apr. 14, 2015. [Online]. Available: https://security.openstack.org/ossa/OSSA-2015-006.html

[6] The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: Aug. 26, 2015. [Online]. Available: https://security. openstack.org/ossa/OSSA-2015-016.html

[7] The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: Feb. 23, 2015. [Online]. Available: https://wiki. openstack.org/wiki/OSSN/OSSN-0025 [9] Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018. [Online]. Available: https://downloads. cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloud- computing-deep-dive.pdf

[8] The OpenStack Project. OpenStack Security Advisories. Accessed: Feb. 2, 2015. [Online]. Available: https://security.openstack.org/ossalist. html

[9] Common Vulnerabilities and Exposures. CVE-2015-5223. Accessed: Jul. 1, 2015. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2015-5223 [11] Common Vulnerabilities and Exposures. CVE-2016-9590. Accessed: Nov. 23, 2016. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2016-9590

[10] Common Vulnerabilities and Exposures. CVE-2016-9590. Accessed: Nov. 23, 2016. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2016-9590.