ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.4

Privacy Protection on Cloud Data

S.Gokul[1], A.Akshai Krishna[2], P.A.Aravind Kumar[3], S.Vijaya Kumar[4]
Student[1, 2, 3], Associate Professor[4]
Department of CSE
R.M.K. Engineering College, India

Abstract:
Frequent item set mining, which is the essential operation in association rule mining, is one of the most widely used data mining techniques on massive datasets nowadays. With the dramatic increase on the scale of datasets collected and stored with cloud services in recent years, it is promising to carry this computation-intensive mining process in the cloud. However, while mining data stored on public clouds, it inevitably introduces privacy concerns on sensitive datasets. In this paper, a new framework for enforcing privacy in frequent item set mining, where data are both collected and mined in an encrypted form in a public cloud service is proposed. Here, three secure frequent item set mining protocols on top of this framework. To guarantee data privacy and computation efficiency, we adopt two different homomorphic encryption schemes and design a secure and effective comparison scheme.

Keywords: Homomorphic Encryption, Two round Search encryption), Top KRetrival, ASP. net, Virtual Private Network, Software Development Kit, Structure Query Language.

I. INTRODUCTION

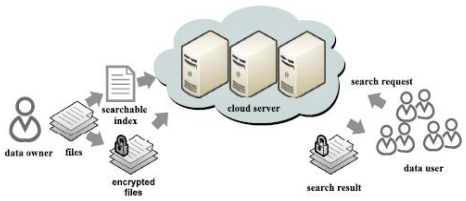
Cloud computing is emerging as a new platform for deploying, managing, and provisioning large-scale services through an Internet-based infrastructure. Successful examples include Amazon EC2, Google App Engine, and Microsoft Azure. As a result, hosting databases in the cloud has become a promising solution for Database-as-a-Service (DaaS) and Web 2.0 applications. In the cloud computing model, the data owner outsources both the data and querying services to the cloud. The data are private assets of the data owner and should be protected against the cloud and querying client; on the other hand, the query might disclose sensitive information of the client and should be protected against the cloud and data owner. Therefore, a vital concern in cloud computing is to protect both data privacy and query privacy among the data owner, the client, and the cloud. The social networking service is one of the sectors that witness such rising concerns. To provide security over cloud, a model is designed which generates OTP, Key Exchange.

II. RELATED WORKS:

Nowadays in many ways security is provided over the data stored in the cloud using various encryption techniques are being used. Security is the major issue that is taken in to considerations to secure the data. Currently no such application is in existence similar to the proposed solution .Since proposed system provide secure over transmission of data over the cloud.

III .PROPOSED SYSYTEM:

3.1. SYSTEM ARCHITECTURE:



3.2.1. NET FRAMEWORK OVERVIEW:

Microsoft's new software development platform, .NET Framework, is the first Microsoft development environment designed from the ground up for Internet development. Although .NET is not meant to be used exclusively for Internet development, its innovations were driven by the limitations of current Internet development tools and technology. The basis of this new development platform consists of three primary components or layers: the common language runtime, the .NET Framework base classes, and the user and program interfaces, as demonstrated in Figure3.2.1.

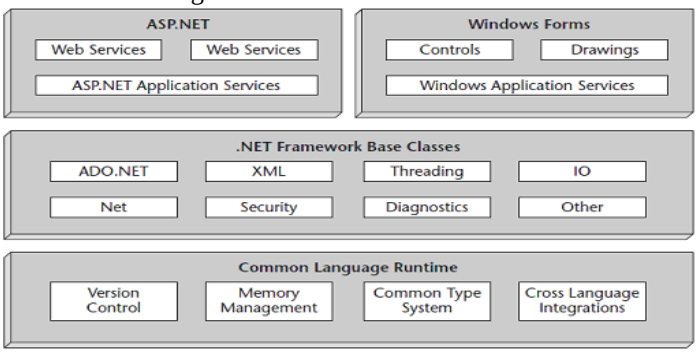


Figure3.2.1. Net Framework Overview

The foundation of the .NET Framework is the common language runtime. Its principal purpose is to load, execute, and manage code that has been compiled to Microsoft's new intermediate byte code format called Intermediate Language (IL). Several languages, notably Microsoft's Visual Basic .NET and C# .NET (pronounced "C sharp"), have compilers supporting this format, and many more are currently in development. It is important to note that the IL code is not interpreted. The common language runtime uses just in time compilers to compile the IL code to native binary code before execution.

3.2.2. NET Framework Class Library: The .NET Framework class library is a collection of reusable classes, or types, that

tightly integrate with the common language runtime. .NET applications benefit from using and extending or inheriting the functionality from the classes and types available in the class library. The class library is very hierarchical and well organized, as shown in Figure 4.2. It starts with the most generic classes and continues to build down to classes with very specific and precise functionality. Although this library is extensive, its organization makes it easy to learn and use. In an age of ever growing technology it is refreshing to see a new technology and a new architecture that promise a reduced learning curve. This model also makes it easy for third party components to be integrated easily with the existing class library.

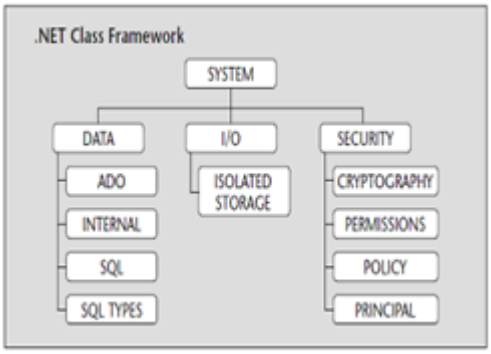


Figure.3.2.2. NET Framework Class Library

3.3.MODULES:

3.3.1. INDEX CREATION MODULE

The data owner has a collection of n files $C = \{f1, f2, \ldots\ldots fn\}$ to outsource onto the cloud server in encrypted form and expects the cloud server to provide keyword retrieval service to data owner himself or other authorized users. To achieve this, the data owner needs to build a searchable index I from a collection of l keywords $W = \{w1, w2, \ldots\ldots wl\}$ extracted out of C, and then outsources both the encrypted index I' file onto the cloud server.

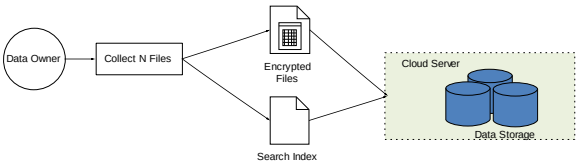


Figure3.3.1. Index Creation Module

3.3.2. DATA ENCRYPTION MODULE:

The encryption module guarantees the operability and security at the same time on server side. Homomorphic encryption allows specific types of computations to be carried out on the corresponding cipher text. The result is the cipher text of the result of the same operations performed on the plaintext. That is, homomorphic encryption allows computation of cipher text without knowing anything about the plaintext to get the correct encrypted result. Fortunately, as a result of employing the vector space model to top-k retrieval, only addition and multiplication operations over integers are needed to compute the relevance scores from the encrypted searchable index. Therefore, can reduce the original homomorphism in a full form to a simplified form that only supports integer operations, which allows more efficiency than the full form does. On the basis of homomorphism property, the encryption scheme can be described as four stages: KeyGen, Encrypt, Evaluate, and Decrypt.

3.3.3. VECTOR SPACE MODULE:

The vector space model to identify the score on multi keyword search against cloud. The vector space model is an algebraic model for representing a file as a vector. Each dimension of the vector corresponds to a separate term, i.e., if a term occurs in the file, its value in the vector is nonzero, otherwise is zero. The vector space model supports multi term and non-binary presentation. Moreover, it allows computing a continuous degree of similarity between queries and files, and then ranking files according to their relevance. It meets our needs of top-k retrieval. A query is also represented as a vector $\vec{q}$ while each dimension of the vector is assigned with 0 or 1 according to whether this term is queried. The score of file f on query $q(score_{f,q})$ is deduced by the inner product of the two vectors: $scores_{f,q} = \vec{v}.\vec{q}$. Given the scores, files can be ranked in order and, therefore, the most relevant files can be found.

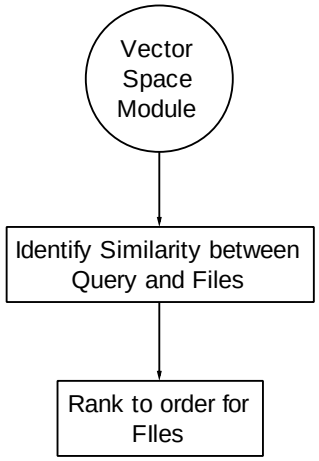


Figure3.3.3. Vector Space Module

.

3.3.4. TOP- K RANK PROVIDE MODULE:

SSE schemes employ server-side ranking based on OPE to improve the efficiency of retrieval over encrypted cloud data. However, server-side ranking based on OPE violates the privacy of sensitive information, which is considered uncompromisable in the security-oriented third party cloud computing scenario, i.e., security cannot be tradeoff for efficiency. To achieve data privacy, ranking has to be left to the user side. Traditional user-side schemes, however, load heavy computational burden and high communication overhead on the user side, due to the interaction between the server and the user including searchable index return and ranking score calculation. A more server-siding scheme might be a better solution to privacy issues.

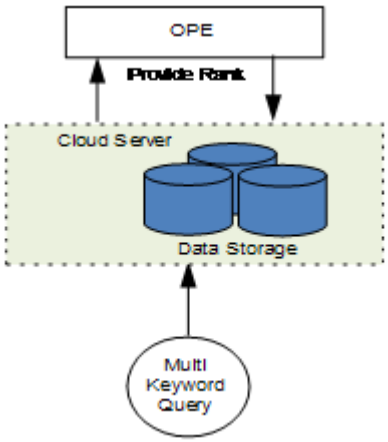


Figure.3.3.3. Top- k rank provide module:

5.2.5 TRSE- QUERY PROCESS MODULE

The cloud server receives a query consisting of multi keywords; it computes the scores from the encrypted index stored on cloud and then returns the encrypted scores of files to the data user. Next, the data user decrypts the scores and picks out the top-k highest scoring files' identifiers to request to the cloud server. The retrieval takes a two-round communication between the cloud server and the data user. The TRSE scheme, in which ranking is done at the user side while scoring calculation is done at the server side.

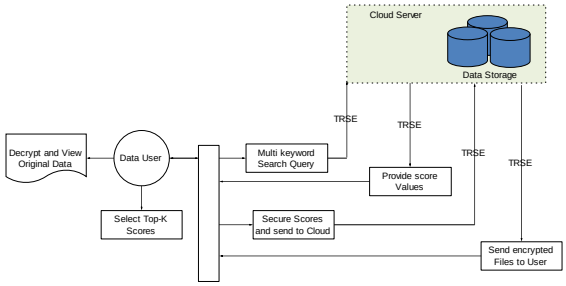
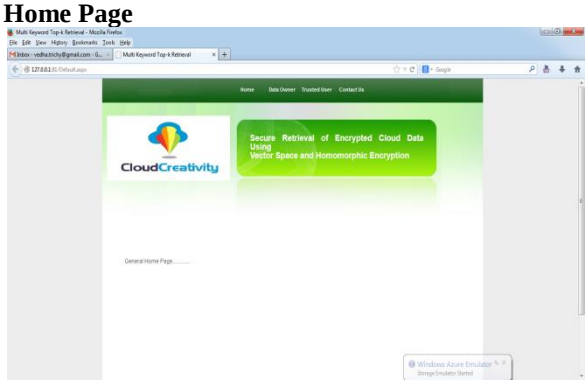


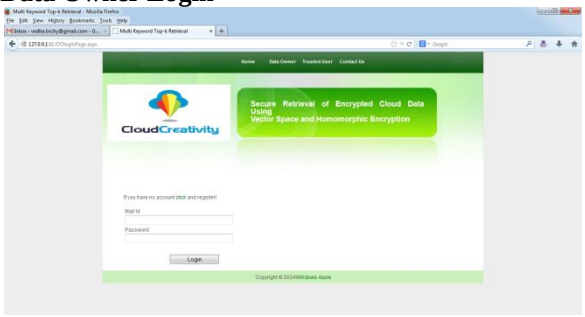
Figure.5.2.5 Trse- Query Process Module

IV .SNAPSHOTS:

Home Page

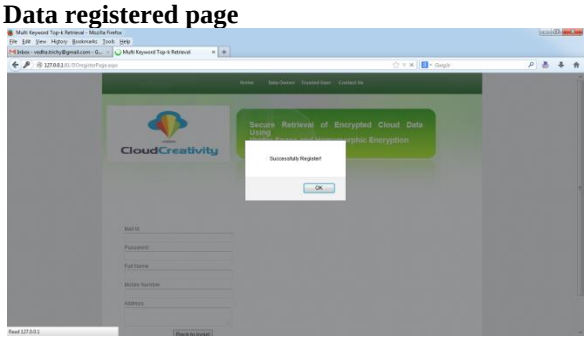


Data Owner Login

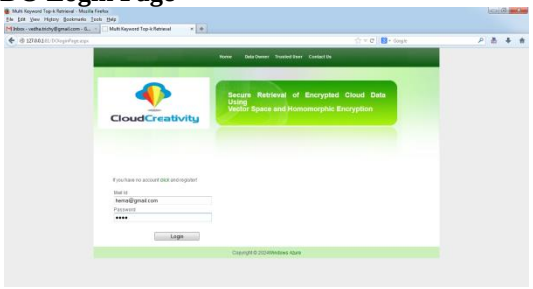


Data Owner Register Page

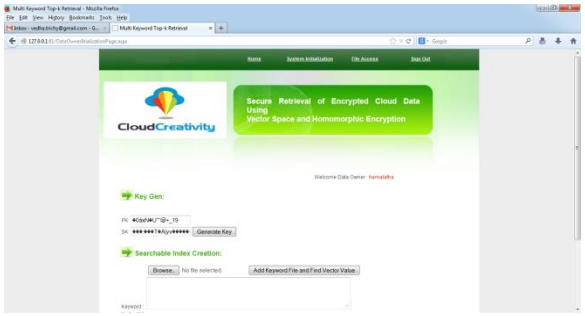
Data registered page



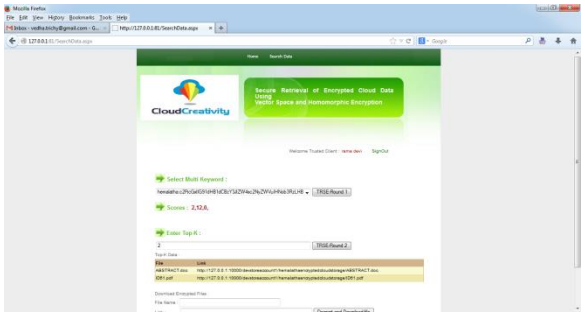
DO Login Page



KEY GENERATION



TRSE-Round 1:



TRSE-Round2

V. CONCLUSION:

Motivate and solve the problem of secure multi keyword top-k retrieval over encrypted cloud data. Based on OPE invisibly

leaking sensitive information, Devise a server-side ranking SSE scheme. We then propose a TRSE scheme employing the fully homomorphic encryption, which fulfils the security requirements of multikeyword top-k retrieval over the encrypted cloud data. By security analysis, we show that the proposed scheme guarantees data privacy.

VI. REFERENCES:

[1]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2].Amazon.com, "Amazon s3 Availability Event: July 20, 2008

[3].AHN, "Romney Hits Obama for Security Information Leakage," http://gantdaily.com/2012/07/25/romney-hits-obama-forsecurity- information-leakage/, 2012. . Cloud Security Alliance, "Top Threats to Cloud Computing," http://www. cloudsecurity alliance.org, 2010.

[4].R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2006.