International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Securing data using Graphical view of Encrypted data

A.Vijetha , K.Mounika Ram , DV.Sravya , U.Narsa Reddy
Assistant Professor in Department of Information Technology .in Teegala Krisha Reddy Engineering college.Telangana
vullojuvijetha@gmail.com
UG Scholar in Department of Information Technology .in Teegala Krisha Reddy Engineering college.Telangana
UG Scholar in Department of Information Technology .in Teegala Krisha Reddy Engineering college.Telangana
UG Scholar in Department of Information Technology .in Teegala Krisha Reddy Engineering college.Telangana

Abstract: *Searchable encryption is an important research area in cloud computing. However, most existing efficient and reliable ciphertext search schemes are based on keywords or shallow syntactic parsing, which are not smart enough to meet with users' search intention. Therefore, in this paper, we propose a content-aware search scheme, which can make syntactic search more smart. First, we introduce conceptual graphs (GRAPHs) as a knowledge representation tool. Then, we present our two schemes (PRSGRAPH and PRSGRAPH-TF) based on GRAPHs according to different scenarios. In order to conduct numerical calculation, we transfer original GRAPHs into their linear form with some modifi- cation and map them to numerical vectors. Second, we employ the technology of multi-keyword ranked search over encrypted cloud data as the basis against two threat models and raise PRSGRAPH and PRSGRAPH-TF to resolve the problem of privacy-preserving smart syntactic search based on GRAPHs. Finally, we choose a real-world data set: CNN data set to test our scheme. We also analyze the privacy and efficiency of proposed schemes in detail. The experiment results show that our proposed schemes are efficient. Index Terms— Searchable encryption, cloud computing, smart syntactic search, conceptual graphs.*

I.INTRODUCTION

Many existing recent schemes are keyword-based search including single keyword and multi-keywords etc. These schemes allow data users to retrieve interested files and return related documents in the encrypted form. However, due to connatural localization of keywords as document eigenvectors, the returned results are always imprecise and unable to satisfy intention of users. That means keywords as a document feature are inadequate data which carry relatively little syntactic information. And some existing schemes hope to explore the relationships among keywords to expand the retrieval results. However, when extracting keywords from documents, the relationships among keywords are out of consideration which leads to the limitation of these schemes. So exploring a new knowledge representation with more syntactic information compared with keywords to realize searchable encryption is a challenging and essential task.

To solve the problem, we introduce Conceptual Graph (GRAPH)
as a knowledge representation tool in this paper. GRAPH is a structure for knowledge representation based on first logic. They are natural, simple and fine-grained syntactic representations to depict texts. A GRAPH is a finite, connected and bipartite graph. We will give a detail description in section 3. However, it's difficult for making match on GRAPH in the encrypted form.One existing representative scheme attempts to solve this problem in the plaintext, but whose process of calculating the similarity scores always relies on the server and external knowledge base. It's unlikely to be realized in the encrypted scenarios, the reason is that the cloud server should learn none of concrete content in our retrieval. Reference proposes a scheme in the encrypted form, but it performs GRAPH homeomorphisms before encrypting. That means the scheme is unable to operate on the encrypted data and doesn't realize searchable encryption in the true sense. Although our previous study is able to realize the goal of performing search on GRAPH, it's an initial and intuitive scheme which is cost expensive and not efficient.

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text ;* encrypted data is referred to as *cipher text*.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Encryption prevents unauthorised access to your data, from emails to WhatsApp messages and bank details, by keeping communication secure between the parties involved.

Cloud computing has been envisioned as the bleeding edge perspective in calculation. In the cloud computing environment, the two applications and assets are passed on ask for over the Internet as services. Cloud is an area of the equipment and programming assets in the server cultivates that give different services over the framework or the Internet to satisfy customer's necessities.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Encryption scrambles text to make it unreadable by anyone other than those with the keys to decode it, and it's becoming less of an added option and more of a must-have element in any security strategy for its ability to slow down and even deter hackers from stealing sensitive information. If good encryption is capable of hindering investigations by FBI experts, consider what it could do for you and your company's sensitive information.

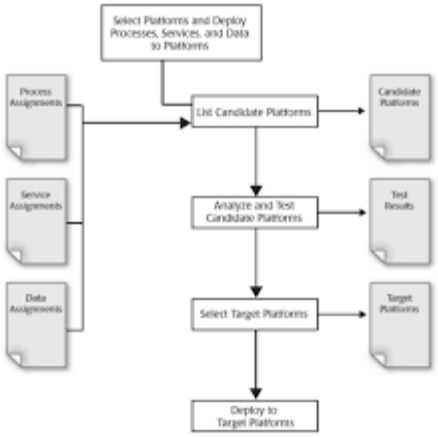

Figure: Cloud graph instance representations.

II.MOTIVATION

Following method adopted for graphical view of data:

Conceptual Graphs as fragmentation to substitute traditional keywords and solve the problem of privacy-preserving smart syntactic search based on conceptual graphs over encrypted outsourced data. Compared with each view, it's more secure and efficient .We consider an non-linear data form of graphs which makes quantitative calculation on conceptual graphs possible. In a sense, we facilitate retrieval on conceptual graphs in syntactic level.e present two practical schemes from different aspects to solve the problem of privacy-preserving smart syntactic search based on conceptual graphs over encrypted outsourced data. They are both secure and efficient, but have their own focus on different aspects.

encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or any other computer network. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. For example, the Payment Card Industry Data Security Standard requires merchants to encrypt customers' payment card data when it is both stored at rest and transmitted across public networks.

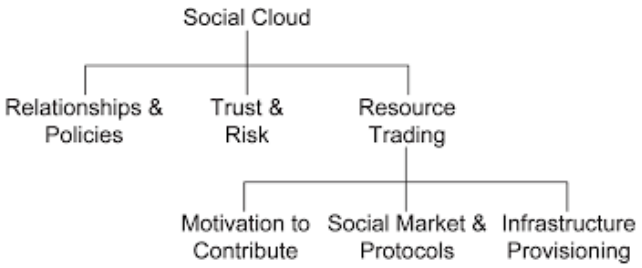

Figure: Types of cloud in graph representation.

In order to achieve the efficient utilization of outsourced encrypted data in syntactic and ranked search under the mentioned threat model, our design must meet the requirement of security and performance as follows.
Syntactic search based on conceptual graphs. To design schemes which can allow perform similarity computation between query GRAPH and source GRAPH and provide ranked results which interest users most effectively.Privacy-preserving. To protect the privacy of users from cloud server, we list some privacy requirement which
schemes must to achieve as follows.

1) Data privacy. That means we should protect documents from the cloud server while keeping available for users. And traditional symmetric cryptography is a good option. We can encrypt the documents by symmetric key cryptography before outsourcing.
2) Index privacy. We must guarantee that the cloud server can't predict the relationship between the documents and "keywords" through the index.
3) "Keyword" privacy. In this paper, we view every part of GRAPH as a "keyword" and the "keyword" is related with each other. So it's important to preserve users' query GRAPH(sentence) and we should generate
secure trapdoors to avoid the leakage of information

about query.

4) Trapdoor unlinkability. When performing search on

the source document, users in nature handle the trap-doors and indexes which are exposed to the cloud server. For the protection of the privacy, we should randomize the trapdoors. And we also should make trapdoors undeterministic so that the same queries in the theory correspond to the different trapdoors. The cloud can't infer the relationship between these trapdoors.

Conventional methods for deleting data permanently from a storage device involve overwriting its whole content with zeros, ones or other patterns – a process which can take a significant amount of time, depending on the capacity and the type of the medium. Cryptography offers a way of making the erasure almost instantaneous. This method is called crypto-shredding. An example implementation of this method can be found on iOS devices, where the cryptographic key is kept in a dedicated 'Effaceable Storage'. Because the key is stored on the same device, this setup on its own does not offer full confidentiality protection in case an unauthorised person gains physical access to the device.

III.PROPOSAL OVER VIEW

The adversary submits two documents set with the same size to a challenger. The challenger runs Setup and generates the secret key The challenger generates a random index with filling a random number "0" or "1" in a random position of index vector. Then the challenger encrypts the random index and sends to the adversary.The adversary follows up the output.

A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle.

Systems get more secure and enterprises adopt more cloud services for which they may only need to manage access to the service, authentication and authorization are growing increasingly important. Ensuring that your enterprise is using the appropriate authentication and authorization processes as the environment and risks change is critical when managing IT security risks.

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

IV. CONCLUSIONS

In this paper, compared with the previous study, we propose two more secure and efficient schemes to solve the problem of privacy-preserving smart syntactic search based on conceptual graphs over encrypted outsourced data. Considering various syntactic representation tools, we select Conceptual Graphs as our syntactic carrier because of its excellent ability of expression and extension. To improve the accuracy of retrieval, we use Tregex simplify the key sentence and make it more generalizable. We transfer GRAPH into its linear form with some modification creatively which makes quantitative calculation on GRAPH and fuzzy retrieval in syntactic level possible. We use different methods to generate indexes and construct two different schemes with two enhanced schemes respectively against two threat models by introducing the frame of DATA. We implement our scheme on the real data set to prove its effectiveness and efficiency. For the further work, we will explore the possibility of syntactic search over encrypted cloud data with natural language processing technology.

REFERENCES

[1]S. Miranda-Jiménez, A. Gelbukh, and G. Sidorov, "Summarizing con-ceptual graphs for automatic summarization task," in Conceptual Struc-
tures for STEM Research and Education. Berlin, Germany: Springer,2013, pp. 245–253.

[2] R. Ferreira, L. de S. Cabral, and R. D. Lins, "Assessing sentence scoringtechniques for extractive text summarization," Expert Syst. Appl., vol. 40,no. 14, pp. 5755–5764, 2013.

[3] M. Liu, R. A. Calvo, A. Aditomo, and L. A. Pizzato, "UsingWikipedia and conceptual graph structures to generate questions for academic writing support," IEEE Trans. Learn. Technol., vol. 5, no. 3, pp. 251–263, Sep. 2012.

[4] M. Heilman and N. A. Smith, "Extracting simplified statements for factual question generation," in Proc. QG 3rd Workshop Question Generat., 2010, pp. 11–20.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.

[6] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. ACNS, 2005, pp. 391–421.

[7] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. ACM CCS, 2006, pp. 79–88. vol. 64, no. 2, pp. 425–437, Feb. 2015.