IMPROVISED SCHEME TO SATISFY THE SECURITY GUARANTEE OF SEARCHABLE SYMMETRIC ENCRYPTION (SSE)

Veeraganti Soumya[1], Chintham Sandeep[2], Sallauddin Mohmmad[3]
[1]Student, M.Tech(CSE), [2,3]Associate Professor
Department of CSE, S R Engineering College, India

ABSTRACT

Presently, searchable file encryption is a warm subject in the field of cloud computing. The existing accomplishments are mostly focused on keyword-based search schemes, and also almost all of them rely on predefined search phrases drawn out in the phases of index construction and also query. Nevertheless, keyword-based search systems overlook the semantic depiction information of customers' access and also can not completely match customers' search intentions. As a result, exactly how to design a content-based search scheme and also make semantic search extra reliable and context-aware is a challenging challenge. In this paper, for the very first time, we define as well as address the issues of semantic search based upon conceptual graphs(CGs) over encrypted outsourced information in clouding computing (SSCG). We firstly use the efficient procedure of "sentence racking up" in message summarization as well as Tregex to extract one of the most crucial and simplified topic sentences from files. We then transform these streamlined sentences into CGs. To perform a measurable estimation of CGs, we develop a new approach that can map CGs to vectors. Next, we rate the returned results based upon the" message summarization score". Furthermore, we suggest a basic idea for SSCG as well as give a substantially enhanced scheme to satisfy the protection assurance of searchable symmetric file encryption (SSE). Ultimately, we pick a real-world dataset-- ie., the CNN dataset to check our plan The results gotten from the experiment reveal the performance of our recommended plan.

Index Terms : *cloud computing, searchable symmetric encryption, conceptual graphs.*

I. INTRODUCTION

What is cloud computing?

Cloud computing is using computing resources (hardware and software) that are supplied as a solution over a network (normally the Internet). The name comes from the common use of a cloud-shaped icon as an abstraction for the complicated infrastructure it has in system layouts. Cloud computer hands over remote services with a customer's information, software as well as computation. Cloud computing contains hardware and software sources offered on the net as managed third-party solutions. These solutions normally offer accessibility to advanced software program applications and high-end networks of server computers.

ISSN: 2005-4238 IJAST

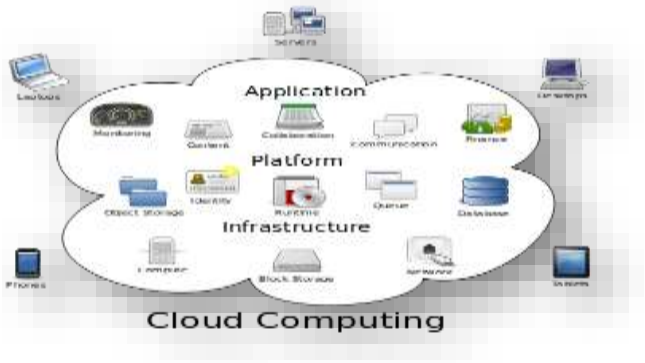


Figure 1 : Cloud computing Structure

How Cloud Computing Works?

The goal of cloud computing is to use conventional supercomputing, or high-performance computing power, usually utilized by army and study centers, to carry out tens of trillions of computations per second, in consumer-oriented applications such as economic portfolios, to provide individualized information, to provide information storage or to power huge, immersive video game.

The cloud computer makes use of networks of big teams of servers generally running affordable customer COMPUTER modern technology with specialized connections to spread out data-processing chores throughout them. This shared IT framework contains huge swimming pools of systems that are linked together. Often, virtualization methods are used to make the best use of the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use

Figure 2 : Cloud computing Characteristics

Services Models:

Cloud Computing comprises three various solution versions, specifically Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three solution designs or layers are finished by an end-user layer that encapsulates the end customer viewpoint on cloud services. The model is displayed in the figure listed below. If a cloud user accesses services on the framework layer, for example, she can run her very own applications on the resources of cloud infrastructure as well as remain responsible for the assistance, maintenance, and safety of these applications herself. If she accesses a solution on the application layer, these jobs are generally looked after by the cloud company.

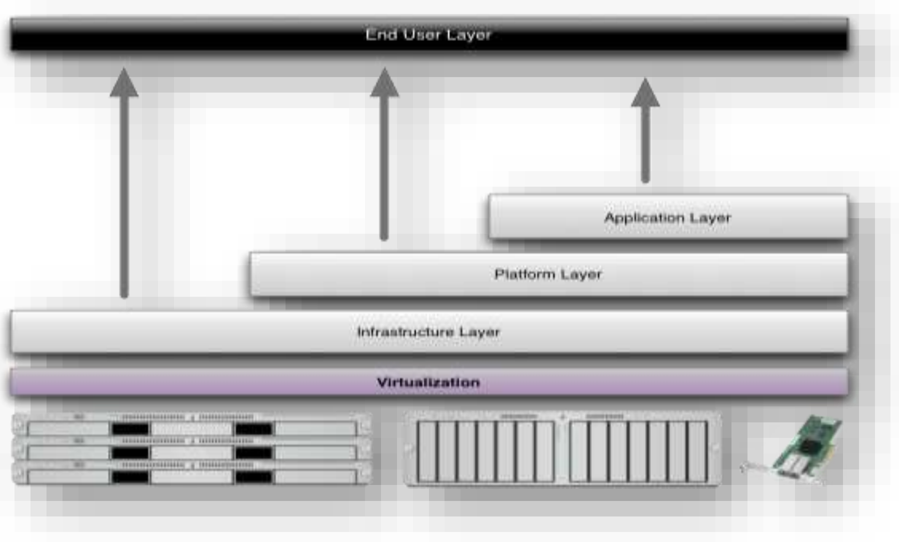


Figure 3 : Service models Structure

II. LITERATURE SURVEY

1) Summarizing conceptual graphs for automatic summarization task

AUTHORS: S.Miranda-Jimnez, A.Gelbukh, and G.Sidorov

We suggest a theoretical graph-based framework for abstractive message summarization. While syntactic or partial semantic representations of texts have been used in literature, total semantic depictions have not been discovered for this purpose. We utilize a complete semantic depiction, particularly, conceptual chart frameworks, composed of concepts as well as theoretical relations. To summarize a conceptual chart, we remove the nodes that represent lesser material, as well as use particular procedures on the resulting smaller conceptual graphs. We determine the value of nodes on heavy conceptual graphs by the HITS formula, enhanced with some heuristics based on VerbNet semantic patterns. Our experimental outcomes are promising.

2) Assessing sentence scoring techniques for extractive text summarization

AUTHORS: R.Ferreira, L.de Souza Cabral, and R.D.Lins

Text summarization is the process of automatically producing a shorter version of several text records. It is an essential means of discovering relevant info in big message libraries or in the Internet. Essentially, text summarization strategies are classified as Extractive and Abstractive. Extractive methods execute message summarization by choosing sentences of papers according to some criteria. Abstractive recaps attempt to enhance the coherence amongst sentences by removing redundancies as well as clarifying the competition of sentences. In terms of extractive summarization, sentence racking up is the strategy most made use of for extractive message summarization. This paper explains and also executes a measurable as well as a qualitative evaluation of 15 formulas for sentence scoring readily available in the literary works. Three different datasets (News, Blogs and Article contexts) were evaluated. In addition, directions to boost the sentence extraction results obtained are recommended.

3) Using wikipedia and conceptual graph structures to generate questions for academic writing support,

AUTHORS: M.Liu, R.Calvo, and A.Aditomo

In this paper, we offer an unique strategy for semiautomatic question generation to support academic writing. Our system initial essences essential phrases from pupils' literature evaluation documents. Each essential phrase is matched with a Wikipedia post and also categorized right into one of 5 abstract principle groups: Research Field, Technology, System, Term, and Other. Using the content of the matched Wikipedia post, the system after that constructs a conceptual graph structure depiction for every essential phrase and also the concerns are after that produced based the framework. To assess the top quality of the computer produced inquiries, we performed a variation of the Bystander Turing examination, which included 20 study students that had composed literature testimonials for an IT methods course. The pedagogical worths of created concerns were reviewed using a semiautomated process. The outcomes indicate that the students had problem comparing computer-generated and also supervisor-generated concerns. Computer-generated questions were likewise rated as being as pedagogically beneficial as supervisor-generated questions, as well as more useful than common inquiries. The findings likewise recommend that the computer-generated questions were more useful for the first-year students than for 2nd or third-year pupils.

4) Extracting simplified statements for factual question generation

AUTHORS: M.Heilman, and N.A.Smith

We address the issue of immediately producing succinct valid concerns from linguistically complicated sentences in reading materials. We review semantic and pragmatic issues that appear in complicated sentences, and after that, we present an algorithm for removing simplified sentences from appositives, secondary provisions, and also other buildings and constructions. We opinion that our method serves as a preliminary action in a bigger question generation procedure. Experimental results show that our approach is better for accurate inquiry generation applications than an alternative text compression algorithm.

III. PROPOSED SYSTEM

➢ In this paper, we solve the trouble of how to make it possible for a searchable file encryption system with the support of semantic expansion. Our work is one of just a few to study rated search over encrypted information represented by CGs in Cloud Computing.
➢ To accomplish our layout objectives for both system security and also use, we divide each CG into three index vectors in action to the structure, the type of concept and the value of the idea of CG. Placed search substantially boosts system functionality by returning the matching data in placed order with regard to certain significance requirements. Thus, to indicate just how the file satisfies the question and rates the returned documents, we make use of the-- "text summarization score" (TSS), which can determine the degree to which the papers match their summarizations according to the relevance rating.
➢ Additionally, if the score is higher, the document is a lot more coincident with the original file. To shield the privacy of the TSS, we after that incorporate order preserving symmetric encryption (OPSE).

IV. IMPLEMENTATION

MODULES:

- Data Owner
- Data User
- Cloud Server
- Conceptual Graph

MODULE DESCRIPTIONS:

Data Owner:

Data owner owns *n* data files $F = \{F1, F2, . . . , Fn\}$ that he encrypts his source documents before they are outsourced to the cloud server. Also, he must guarantee that these documents can be searched effectively. In this paper, the data owner encrypts their documents set and generates searchable indexes before outsourcing data to the cloud server. Besides this, the pre-process work such as the construction of CG, the transformation of CG into vectors and the update operation of documents should be handled ahead of time. The data user also should make a secure distribution of the key information of trapdoor generation and provide authorization for authorized data users.

Data User:

Data users should obtain a warrant from data owner to have access to documents. Data users should submit a simple sentence to generate a trapdoor and take back the documents which meet his requirement from the cloud server.

Cloud Server:

Cloud server receives the store request from the data owner and executes the operation of storing the encrypted documents and searchable indexes. When the data users send the trapdoor to the cloud server, the cloud server makes a computation of relevance scores and returns top-k related documents to the data users. The cloud server is also responsible for executing the command of updating documents and searchable indexes.

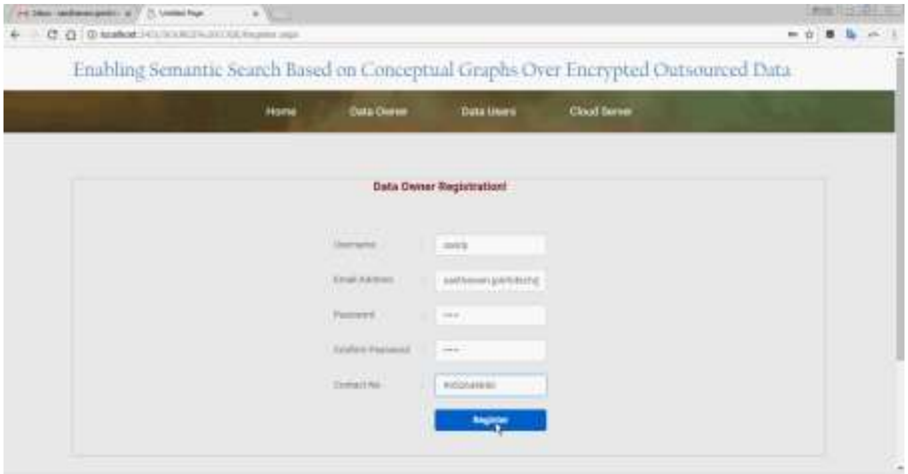
Conceptual Graph:

Conceptual graph is defined as a graph representation of logic that is based on the semantic networks of Artificial Intelligence (AI) and existential graphs. There are usually two types of nodes: concepts (rectangles) and conceptual relations (ovals). A concept is connected with another concept by a conceptual relation. Each conceptual relation must be connected to some other concepts. For each CG, we denoted conceptual relations as semantic roles, with 30 relations approximately including 6 tenses. In this paper, we choose approximately 24 relations, regardless of tenses.

V. RESULTS

Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data
Home
Data Owner
Data Users
Cloud Server
CLOUD COMPUTING
Abstract

Figure 4 : Home page

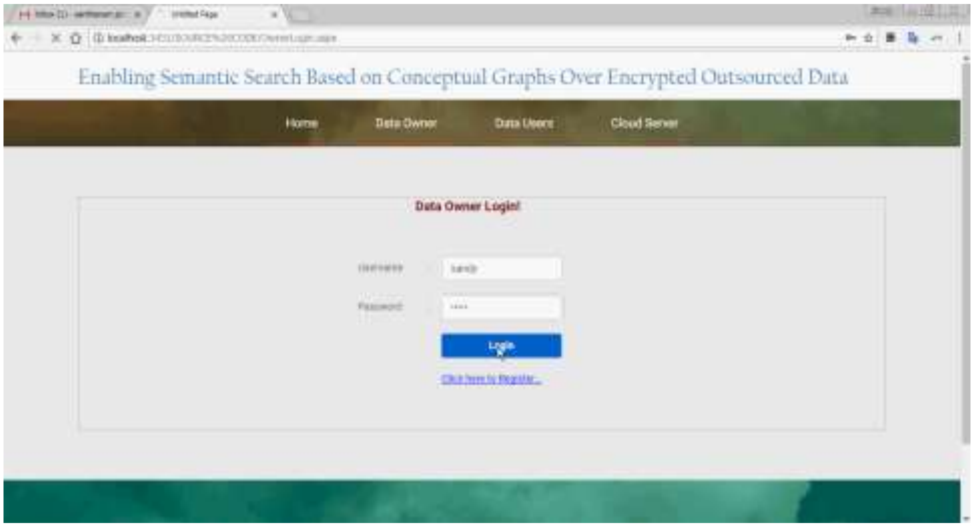


Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Data Owner Registration!

Username	[illegible]
Email Address	[illegible]
Password	••••
Confirm Password	••••
Contact No	[illegible]

Figure 5 : Owner Registration

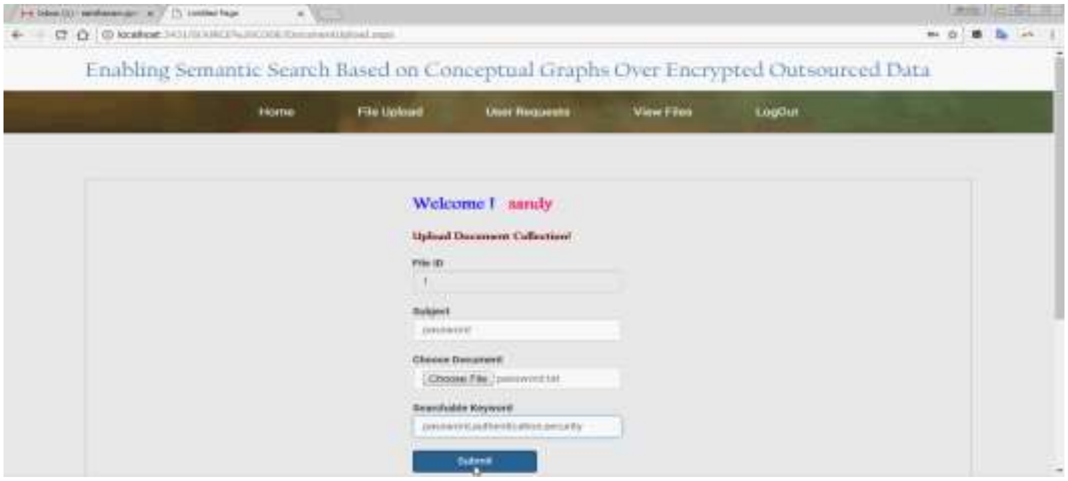


Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Data Owner Login!

Username	[illegible]
Password	••••

Figure 6 : Owner Login



Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Welcome ! sandy

Upload Document Collection!

File ID

1

Subject

password

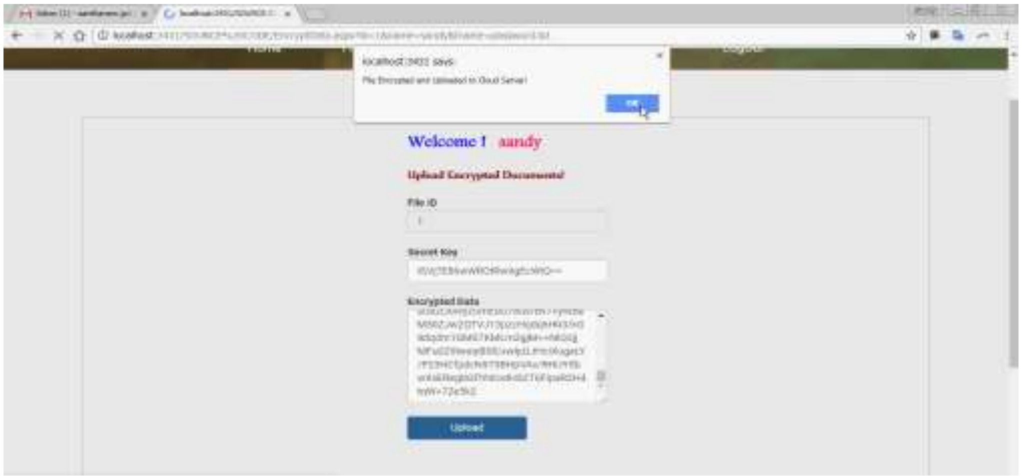
Choose Document

password.txt

Searchable Keyword

password,authentication,security

Figure 7 : Upload Document



localhost:3431 says:

File Encrypted and Uploaded to Cloud Server!

Welcome ! sandy

Upload Encrypted Documents!

File ID

1

Secret Key

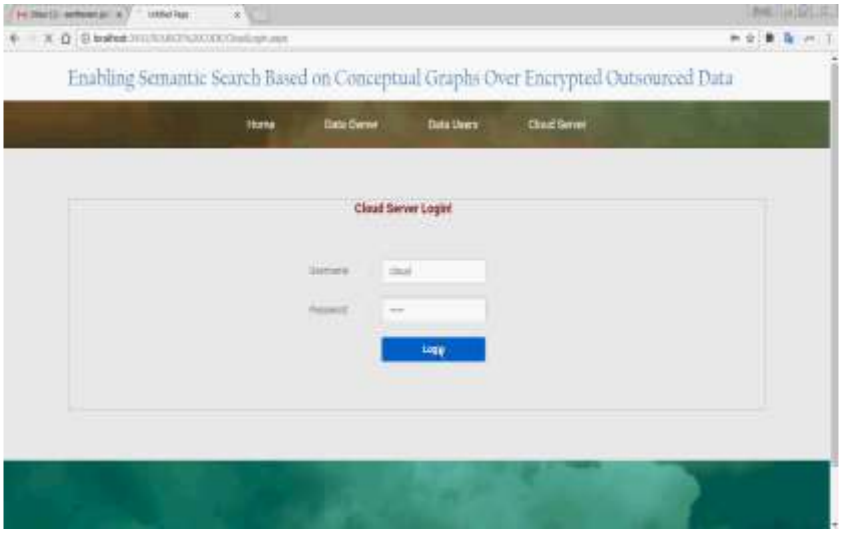
[illegible]

Encrypted Data

[illegible]

Figure 8 : Upload Encrypted Documents

ISSN: 2005-4238 IJAST



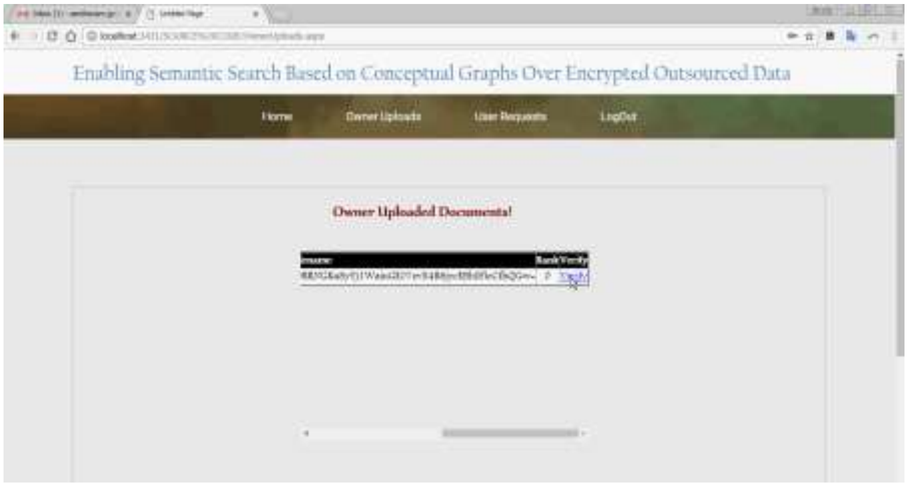
Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Cloud Server Login!

Username: cloud

Password: ****

Figure 9 : Cloud Server Login

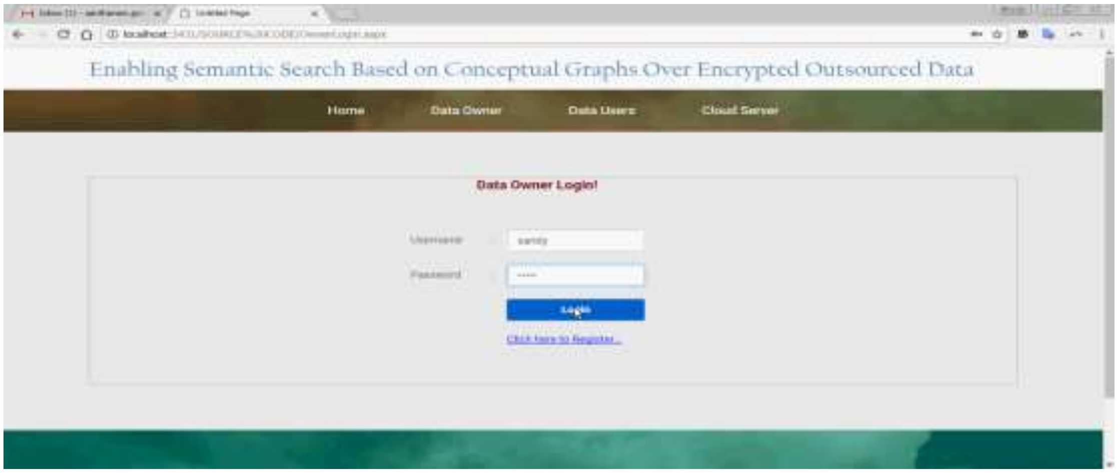


Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Owner Uploaded Documents!

fname	Rank	Verify
[illegible]	0	Verify

Figure 10: Owner uploaded Document

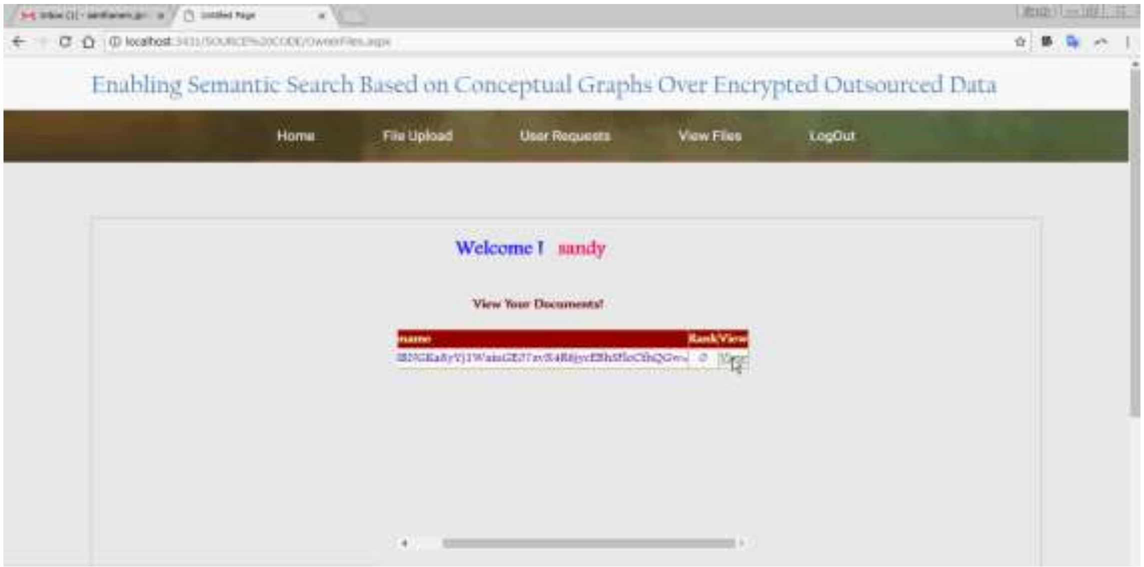

Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data
Home
Data Owner
Data Users
Cloud Server
Login
Click here to Register..

Data Owner Login!

Username : sandy

Password : •••••

Figure 11 : Data Owner Login


Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data
Home
File Upload
User Requests
View Files
LogOut

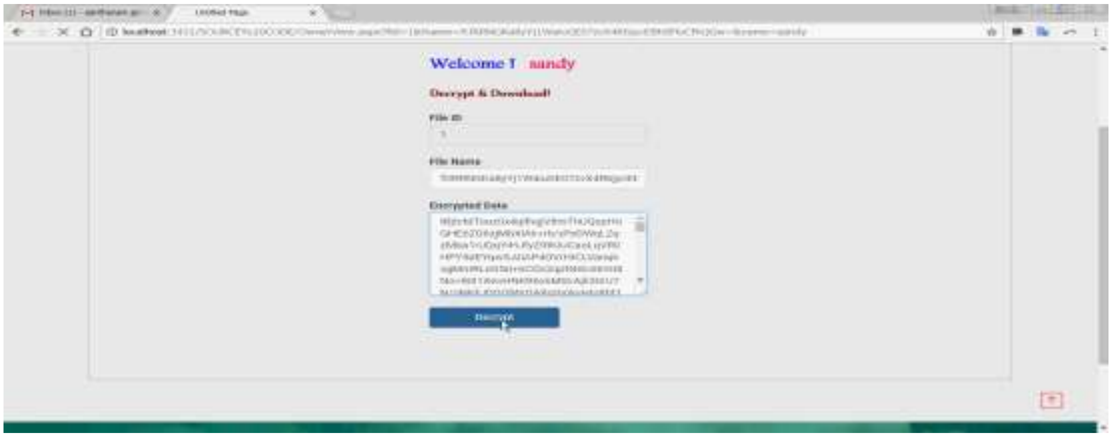
Welcome ! sandy

View Your Documents!

name	Rank	View
BNGKa8yVj1WaiuGE77nvS4R8jycEBhSfloCfhQGw	0	View

Figure 12 : View Documents

ISSN: 2005-4238 IJAST



Welcome ! sandy

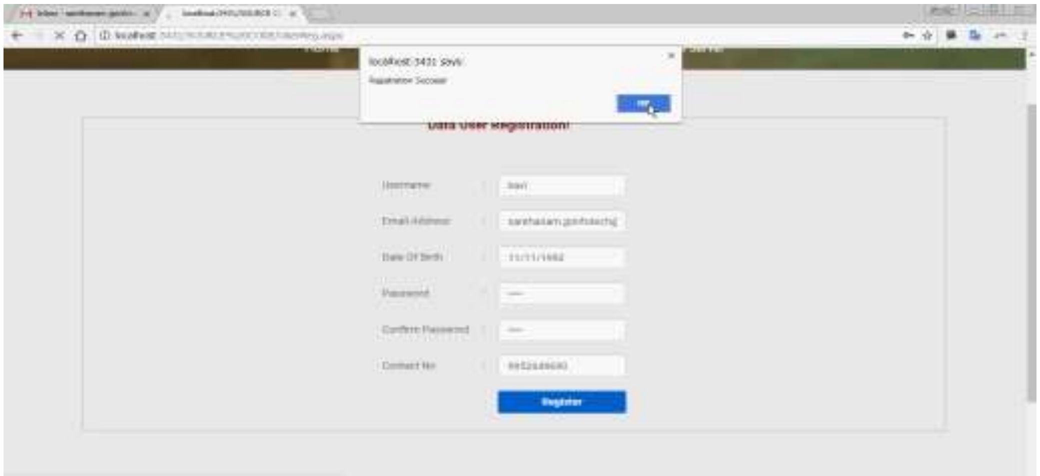
Decrypt & Download!

File ID: 1

File Name: [illegible]

Encrypted Data: [illegible]

Figure 13 : Decrypt and Download



localhost:3431 says

Registration Success

Data User Registration!

Username : Ravi

Email Address : sarehalam.pinfotech[illegible]

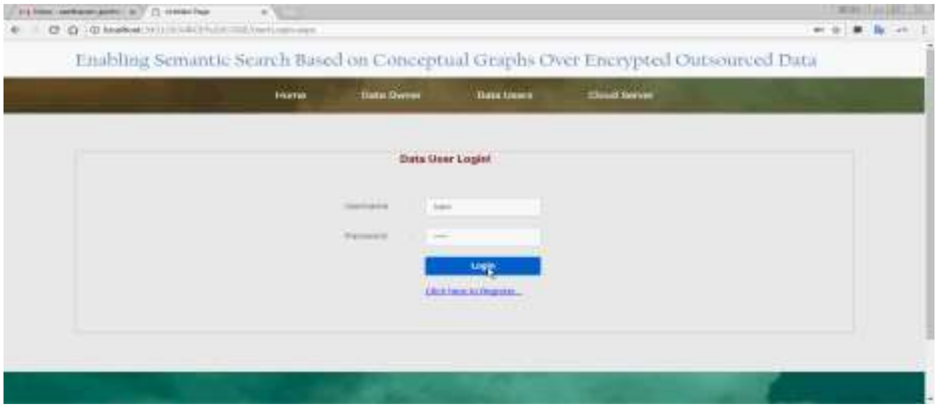
Date Of Birth : 11/11/1992

Password : ----

Confirm Password : ----

Contact No : [illegible]

Figure 14 : Registration



Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

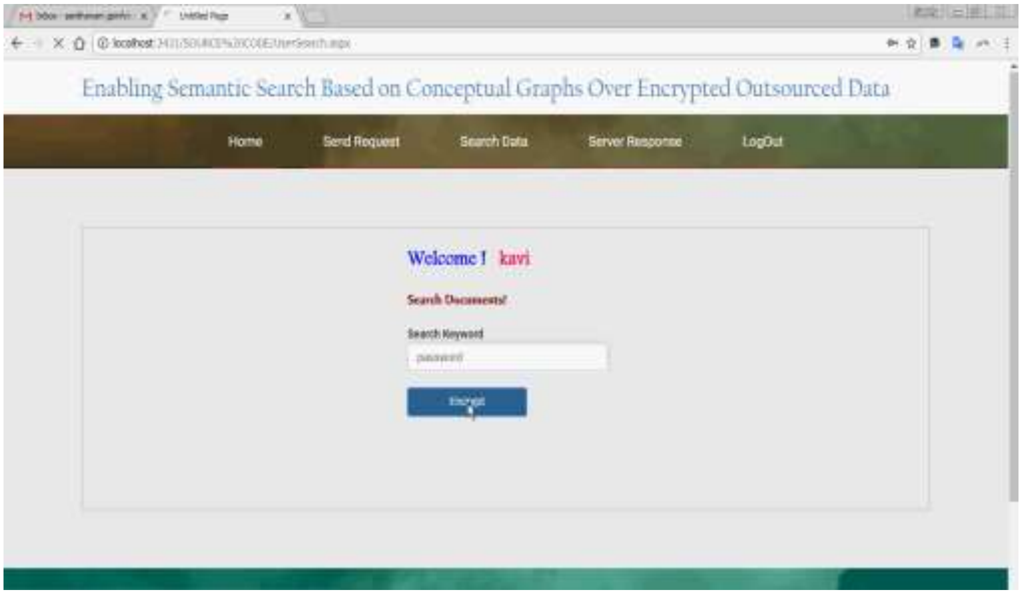
Data User Login!

Username : Ravi

Password : ----

Figure 15 : Data User login

ISSN: 2005-4238 IJAST



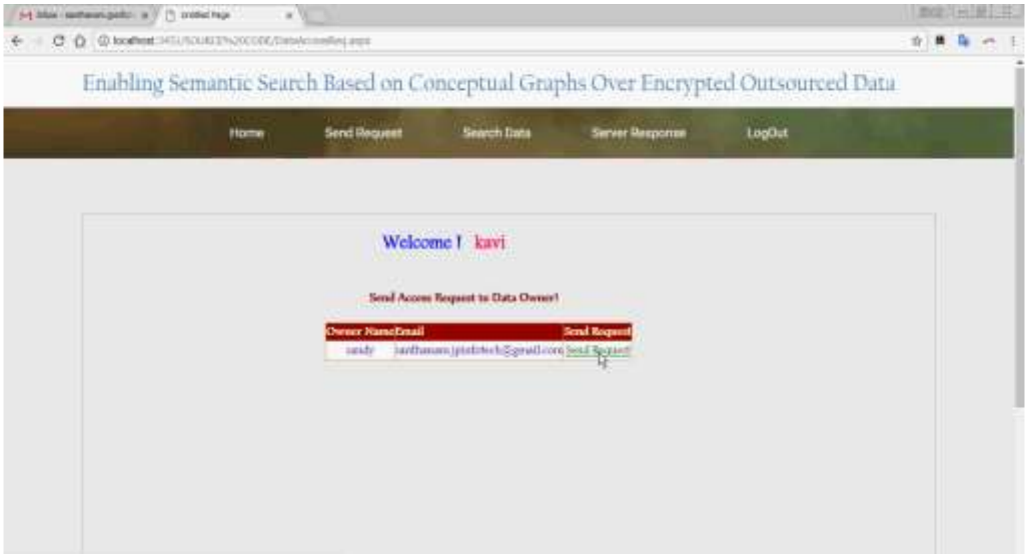
Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Welcome ! kavi

Search Documents!

Search Keyword: password

Figure 16 : Search Keyword



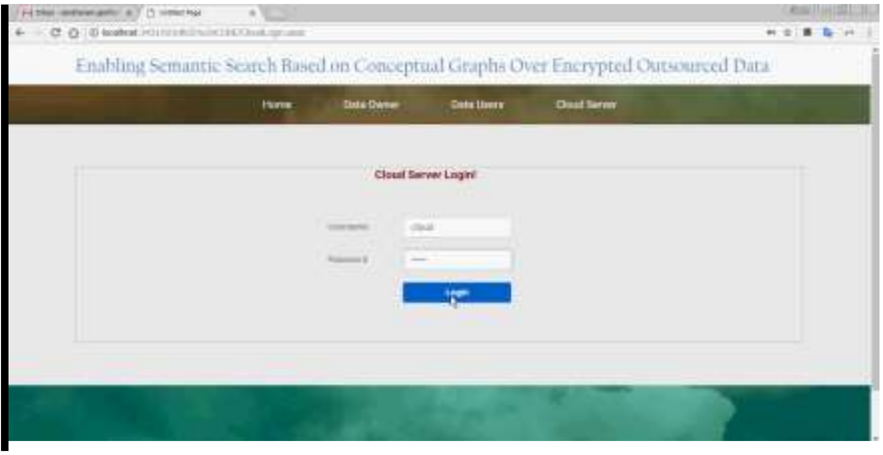
Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Welcome ! kavi

Send Access Request to Data Owner!

Owner Name	Email	Send Request
sandy	santhanam.jpinfotech@gmail.com	Send Request

Figure 17 : Sending access report to Data Owner



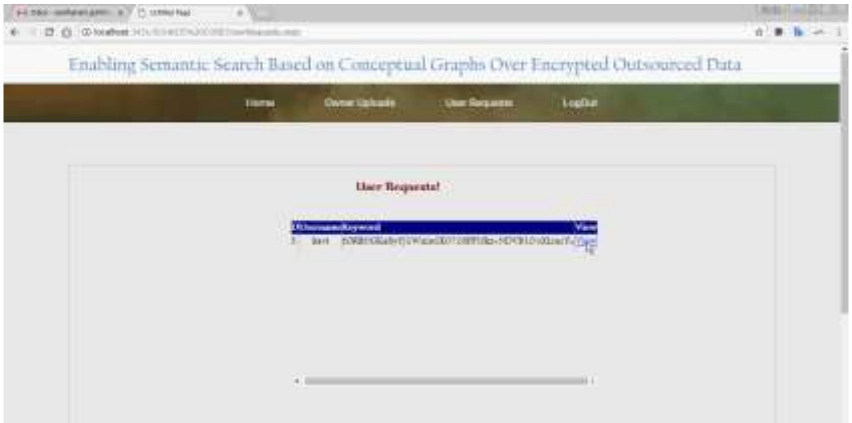
Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Cloud Server Login!

Username: cloud

Password: -----

Figure 18 : Cloud Server Login

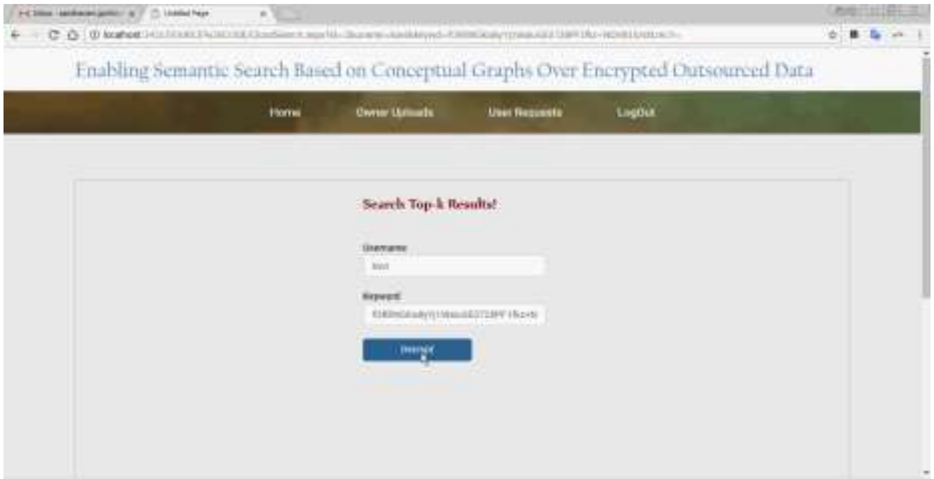


Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

User Requests!

ID	Username	Keyword	View
3	test	[illegible]	Open

Figure 19 : User requests



Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Search Top-k Results!

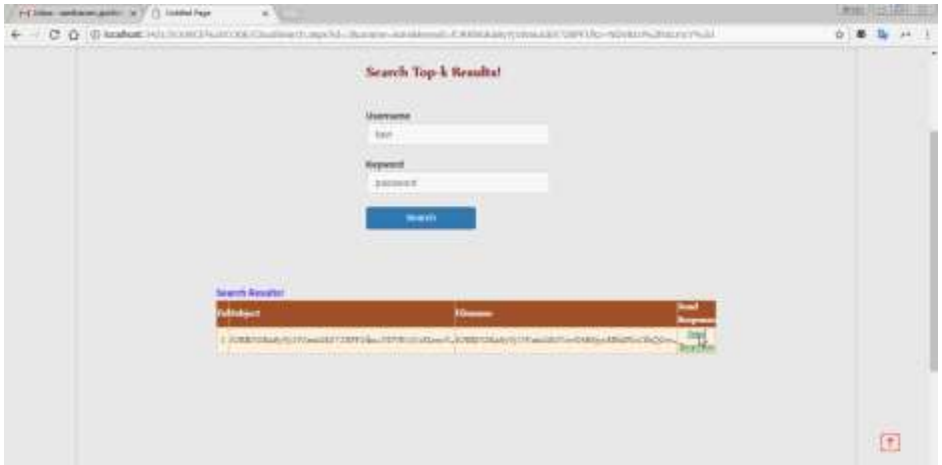
Username

test

Keyword

[illegible]

Figure 20 : Search Top-k Results



Search Top-k Results!

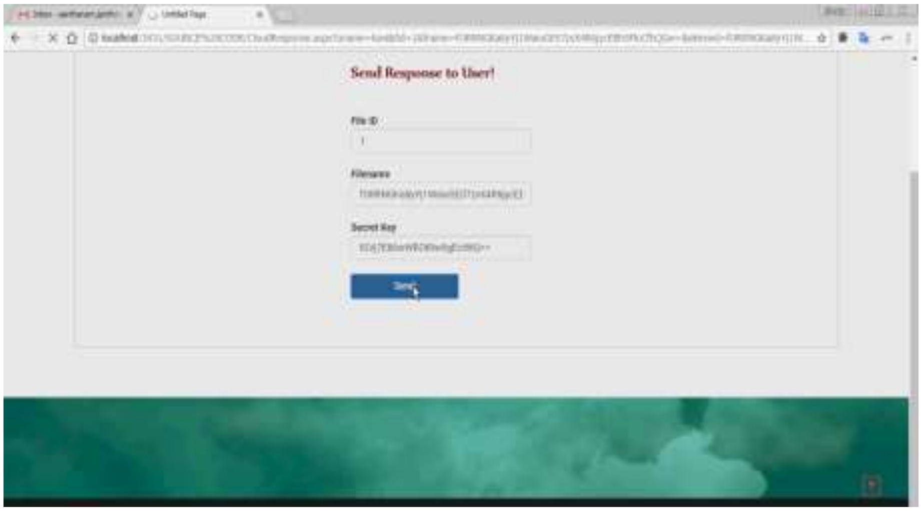
Username
[illegible]

Keyword
password

Search Results!

[illegible]	Filename	Send Response
1 [illegible]	[illegible]	Send Response

Figure 21



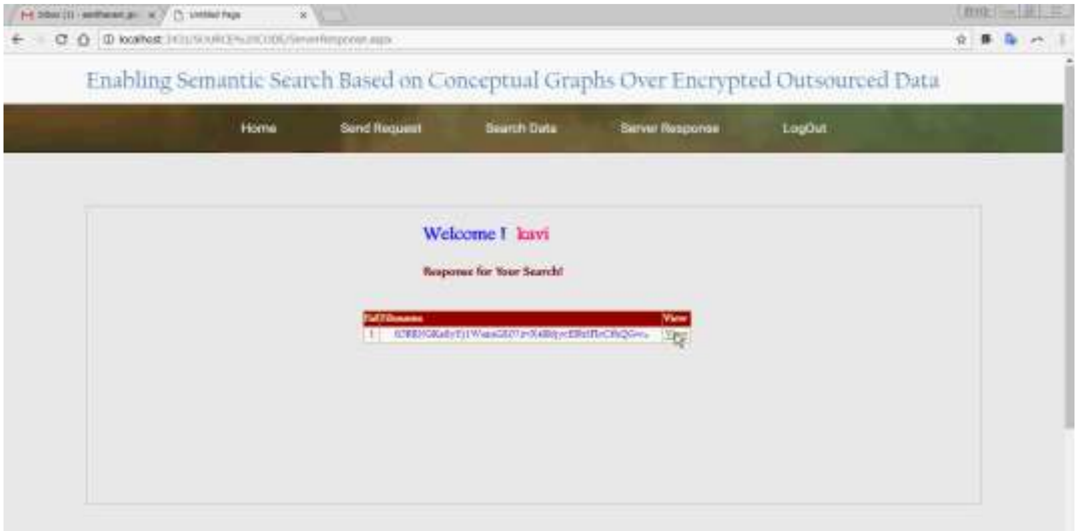
Send Response to User!

File ID
1

Filename
[illegible]

Secret Key
[illegible]

Figure 22 : Send response to User



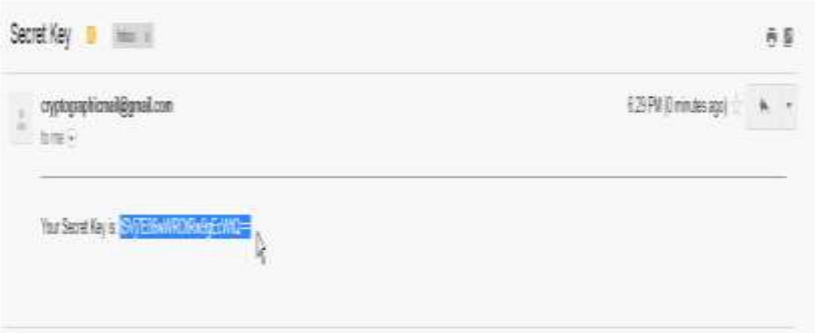
Enabling Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Welcome ! kavi

Response for Your Search!

FileID	Filename	View
1	[illegible]	View

Figure 23 : Response for the search



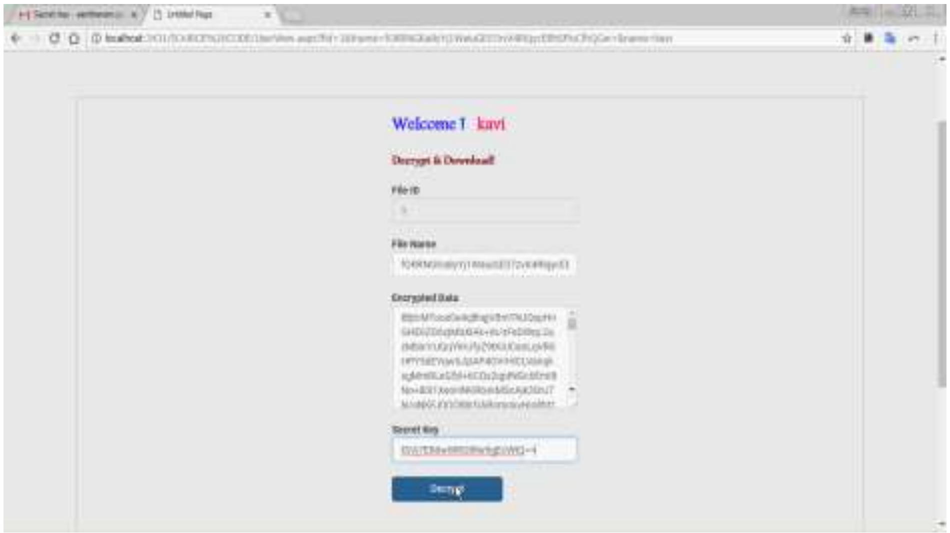
Secret Key

cryptographicmail@gmail.com
to me

6:29 PM (0 minutes ago)

Your Secret Key is [illegible]

Figure 24 : Secret Key



Welcome ! kavi

Decrypt & Download!

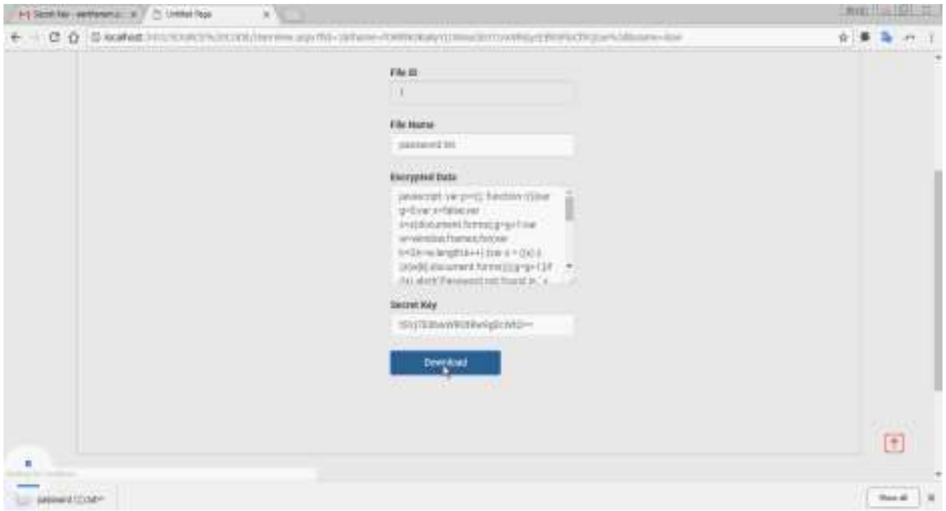
File ID
1

File Name
[illegible]

Encrypted Data
[illegible]

Secret Key
[illegible]

Figure 25 : Decrypt and Download



File ID
1

File Name
password.txt

Encrypted Data
[illegible]

Secret Key
[illegible]

Figure 26 : Result

VI. CONCLUSION

In this paper, we define the problem of semantic search based on conceptual graphs over encrypted outsourced data for the very first time. We select CGs amongst various methods of understanding depiction to represent the documents. To generate the CGs, we apply a state-of-the-art technique, ie., message summarization and also Tregex a tool for streamlining sentences in our technique. And to achieve our design objectives of both system safety and also usability, we separate each CG into three index vectors based on the framework of the CG, the kind of concept as well as the value of principle. We use order-preserving symmetrical file encryption to our scheme to enhance safety. Speculative outcomes show the efficiency of our suggested scheme. In more work, we will continue to research the semantic search over encrypted cloud data with the assistance of natural language processing modern technology. Specifically, we are considering presenting various other semantic depictions in encrypted kind or changing the procedure of changing a conceptual graph into a mathematical vector which can assist improve accuracy as well as performance.

REFERENCES

[1] S.Miranda-Jimnez, A.Gelbukh, and G.Sidorov, ”Summarizing conceptual graphs for automatic summarization task,” Conceptual Structures for STEM Research and Education,Springer Berlin Heidelberg, pp. 245-253,2013.

[2] R.Ferreira, L.de Souza Cabral, and R.D.Lins, ”Assessing sentence scoring techniques for extractive text summarization,” Expert systems with applications,vol.40,no.14,pp.5755-5764,2013.

[3] M.Liu, R.Calvo, and A.Aditomo, ”Using wikipedia and conceptual graph structures to generate questions for academic writing support,” Learning Technologies,IEEE Transactions on,vol.5,no.3,pp.251-263,2012.

[4] M.Heilman, and N.A.Smith, ”Extracting simplified statements for factual question generation ,” Proceedings of QG2010: The Third Workshop on Question Generation,pp.11-20,2010.

[5] D.X.Song, D.Wagner, and A.Perrig, ”Practical techniques for searches on encrypted data,” Proceedings of Security and Privacy,2000 IEEE Symposium on,pp.44-55,2000.

[6] Y.-C.Chang and M.Mitzenmacher, ”Privacy preserving keyword searches on remote encrypted data,” Proceedings of ACNS,pp.391-421,2005.

[7] R.Curtmola, J.A.Garay, S.Kamara, and R.Ostrovsky, ”Searchable symmetric encryption: improved definitions and efficient constructions,” Proceedings of ACM CCS,pp.79-88,2006.

[8] C.Wang, N.Cao, and J.Li, ”Secure ranked keyword search over encrypted cloud data,” Proceedings of Distributed Computing Systems (ICDCS),2010 IEEE 30th International Conference on,pp.253-262,2010.

[9] N.Cao, C.Wang, and M.Li, ”Privacy-preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Distributed Systems, IEEE Transactions on,vol.25,no.1,pp.222-233,2014.

[10] W.Sun, B.Wang, and N.Cao, ”Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” Proceedings of the 8th ACM SIGSAC symposium on Information,computer and communications security,pp.71-82,2013.

[11] R.Li, Z.Xu, and W.Kang, ”Efficient multi-keyword ranked query over encrypted data in cloud computing,” Future Generation Computer Systems,vol.30,pp.179-190,2014.

[12] Z.Fu, X.Sun, and Q.Liu, ” Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing,” IEICE Transactions on Communications, vol.98,no.1,pp.190-200,2015.

[13] Z.Xia, X.Wang, and X.Sun, ”A Secure and Dynamic Multikeyword Ranked Search Scheme over Encrypted Cloud Data,”Parallel and Distributed Systems,IEEE Transactions on, vo.27,no.2,pp.340-352,2015.

[14] Z.Fu, J.Shu, and X.Sun, ”Semantic keyword search based on trie over encrypted cloud data,” Proceedings of the 2nd international workshop on Security in cloud computing,ACM, pp.59-62,2014.

[15] J.F.Sowa, ”Conceptual structures: information processing in mind and machine,” 1983.

[16] J.F.Sowa, Conceptual Graphs. In: Handbook of Knowledge Representation,pp.213-237,2008.

[17] J.Zhong, H.Zhu, and J.Li, Conceptual graph matching for semantic search. Conceptual structures: Integration and interfaces,Springer Berlin Heidelberg,pp.92-106,2002.

[18] G.S.Poh, M.S.Mohamad, and M.R.Zaba, Structured encryption for conceptual graphs. Advances in Information and Computer Security. Springer Berlin Heidelberg,pp.105-122,2012.

[19] S.Hensman, and J.Dunnion, ”Automatically building conceptual graphs using VerbNet and WordNet,” Proceedings of the 2004 international symposium on Information and communication technologies, Trinity College Dublin,pp.115-120,2004.

[20] W.K.Wong, D.W.Cheung, and B.Kao, ”Secure KNN computation on encrypted databases,” Proceedings of the 2009 ACM SIGMOD International Conference on Management of data,pp.139-152,2009.

[21] A.Boldyreva, N.Chenette, and Y. Lee, Order-preserving symmetric encryption.Advances in Cryptology-EUROCRYPT 2009, Springer Berlin Heidelberg, pp. 224-241,2009.

[22] Z.Fu, K.Ren, and J.Shu, ”Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement,” Parallel and Distributed Systems,IEEE Transactions on, 2015.

[23] J. Wang, X. Chen,and X. Huang, ”Verifiable auditing for outsourced database in cloud computing,” IEEE Transactions on Computers,vol.64,no.11,pp.3293-3303,2015.

[24] F. Cheng, Q. Wang,and Q. Zhang, ”Highly Efficient Indexing for Privacy-Preserving Multi-keyword Query over Encrypted Cloud Data,” International Conference on Web-Age Information Management,pp.348-359,2014.