Multi Ranked Semantic Keyword Search with Access Control in Dynamic Cloud Environments

Kowtham. P R M

EGS Pillay Engineering College, Nagapattinam

ABSTRACT

With the explosive growth of data volume in the cloud computing environment, data owners are increasingly inclined to store their data on the cloud. Although data outsourcing reduces computation and storage costs for them, it inevitably brings new security and privacy concerns, as the data owners lose direct control of sensitive data. Meanwhile, most of the existing ranked keyword search schemes mainly focus on enriching search efficiency or functionality, but lack of providing efficient access control and formal security analysis simultaneously. To address these limitations, in this paper we propose an multi data owner scheme can be implement in cloud storage, using Fuzzy search and rank the data based on keyword search.

Key Words: Cloud computing, ranked keyword search,access control, fuzzy search, ECC based algorithm.

INTRODUCTION

In today’s data intensive world, cloud computing is new type of computing paradigm which enables sharing of computing resources over the internet. The cloud characteristics are on-demand self-service, location independent network access, ubiquitous network access and usage-based pay. Due to these charming features private and public organization are outsourcing their large amount of data on cloud storage. Organizations are motivated to migrate their data from local site to central commercial public cloud server. By outsourcing data on cloud users gets relief from storage maintenance. Although there are many benefits to migrate data on cloud storage it brings many security problems. Therefore, the data owners hesitate to migrate the sensitive data. In this case the control of data is going towards cloud service provider. This security problem induces data owners to encrypt data at client side and outsource the data. By encrypting data improves the data security but the data efficiency is decreased because searching on encrypted data is difficult.

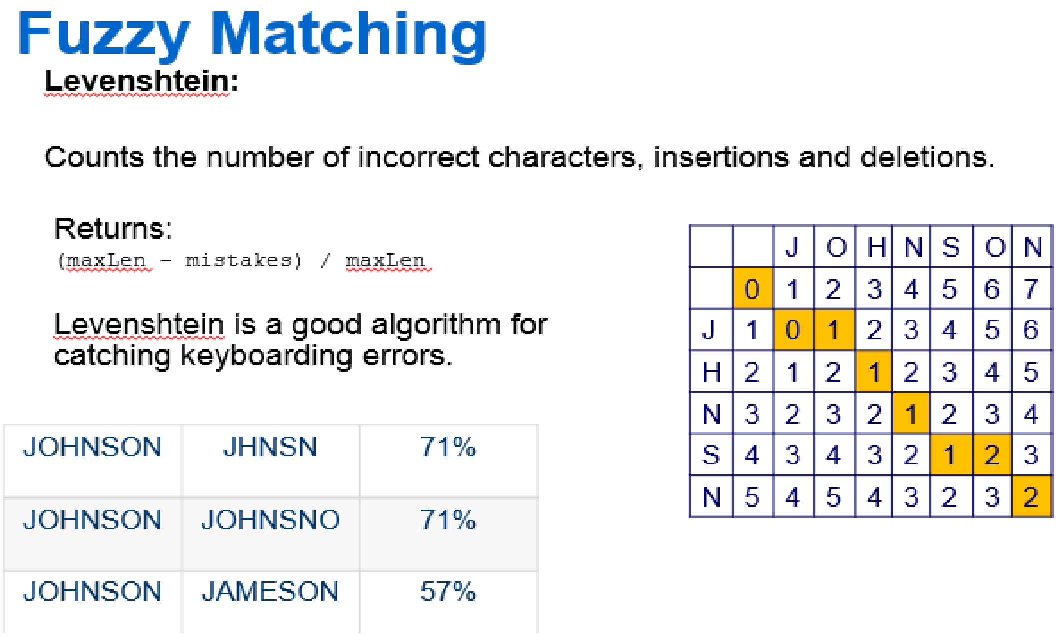
Problem Formulation

The problem that is identified in this project are noted below:

- Difficult to extract data in encrypted cloud storage.
- Multiple keywords can’t be analyzed.
- Limited authentication can be used.
- Symmetric encryption level security.
- Provide the irrelevant results at the time of data retrieval.

TECHNOLOGY TO BE USED FOR THE SOLUTION

```
1.ECC ENCRYPTION
Input: Parameters from the elliptic curve domain (p, E, P, n), Public Key Q,
Raw Text m Output: Encrypted text (C1, C2) begin
1. Represent the message m as a point M in E(Fp)
2. Select k ∈R[1,n−1].
3. Calculate C1 = kP
4. Calculate C2 = M + kQ.
5. Return (C1, C2) end.
2. ECC DECRYPTION
Input: Parameters from the elliptic curve domain (p, E, P, n), Private key d, Encrypted text (C1, C2)
Output: Raw Text m begin
1. Calculate M = C2- dC1 and extract m from M.
2. Return (m) end.
```



Fuzzy Matching

Levenshtein:

Counts the number of incorrect characters, insertions and deletions.

Returns:
(maxLen - mistakes) / maxLen

Levenshtein is a good algorithm for catching keyboarding errors.

JOHNSON	JHNSN	71%
JOHNSON	JOHNSNO	71%
JOHNSON	JAMESON	57%

		J	O	H	N	S	O	N
	0	1	2	3	4	5	6	7
J	1	0	1	2	3	4	5	6
H	2	1	2	1	2	3	4	5
N	3	2	3	2	1	2	3	4
S	4	3	4	3	2	1	2	3
N	5	4	5	4	3	2	3	2

How to imply hardware and software usage

HARDWARE REQUIREMENTS

Processor	: Intel processor 2.6.0 GHZ
RAM	: 2GB
Hard disk	: 160 GB
Compact Disk	: 650 Mb
Keyboard	: Standard keyboard
Monitor	:15-inch color monitor

SOFTWARE REQUIREMENTS

• Operating System	: Windows OS
• Front End	: ASP.NET
• Back End	: SQL SERVER
• IDE	: VISUAL STUDIO

EXPECTED OUTCOME

- Design the cloud framework for multi data owners for extract the relevant data from encrypted storage
- Fuzzy based approach to construct index vectors and rank the index based on search
- Efficient and semantic based keyword search
- Verification scheme for outsourced cloud storage

PROPOSED SOLUTION

- Multi data owner scheme can be implemented in cloud storage
- Semantic search for retrieving documents using **fuzzy search** and rank the data based on keyword search
- Implement **ECC based algorithm** to encrypt the cloud data
- Authentication scheme can be implemented in terms of **Aadhar Card verification.**

CONCLUSION

- Retrieve large number of relevant documents based on user searchable keyword
- Anonymous access can be blocked
- Mapping can be done in encrypted cloud storage
- Easy to analyze relationship between multi keywords

REFERENCES

C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, Aug 2012.

Jiayi Li, Jianfeng Ma, Yinbin Miao, Ruikang Yang, and Ximeng Liu, "Practical Multi-Keyword Ranked search with Access Control Over Encrypted Cloud Data,"IEEE Transactions on Cloud Computing, vol. 10, no. 3, 01 July-September 2022.