Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 06, June -2018

"AN EFFICIENT AND FINE-GRAINED BIG DATA ACCESS CONTROL SCHEME WITH PRIVACY-PRESERVING POLICY"

[1]Mayur Jundare, [2]Harshal Ramesh Chandanshive,
[3]Sagar Hake, [4]Om Jaiswal,
[5]Prof.Avinash Devare

[1]*Sinhgad academy of engineering, Department of Computer Engineering ,Pune*
[2]*Sinhgad academy of engineering, Department of Computer Engineering ,Pune*
[3]*Sinhgad academy of engineering, Department of Computer Engineering ,Pune*
[4]*Sinhgad academy of engineering, Department of Computer Engineering ,Pune*
[5]*Sinhgad academy of engineering, Department of Computer Engineering ,Pune*

Abstract : *Instructions to control the entrance of the enormous measure of huge information turns into an exceptionally difficult issue, particularly when huge information are put away in the cloud. Ciphertext-Policy Attribute based Encryption (CP-ABE) is a promising encryption procedure that empowers end-clients to encode their information under the entrance approaches characterized over a few characteristics of information shoppers and finely permits information customers whose qualities fulfill the entrance strategies to unscramble the information. In CP-ABE, the entrance strategy is connected to the ciphertext in plaintext shape, which may likewise release some private data about end-clients. Existing techniques just halfway shroud the property estimations in the entrance approaches, while the trait names are as yet unprotected. In this paper, we propose a proficient and fine-grained huge information get to control conspire with protection safeguarding arrangement. In particular, we shroud the entire characteristic (as opposed to just its qualities) in the entrance arrangements. To help information unscrambling, we additionally plan a novel Attribute Bloom Filter to assess whether a property is in the entrance arrangement and find the correct position in the entrance approach on the off chance that it is in the entrance strategy. Security examination and execution assessment demonstrate that our plan can save the protection from any LSSS get to arrangement without utilizing much overhead.*

Keywords*: Searchable encryption, Multi-keyword ,Fine-grained, Cloud computing.*

I. INTRODUCTION

In the period of huge information, an immense measure of information can be produced rapidly from different sources (e.g., advanced cells, sensors, machines, interpersonal organizations, and so forth.). Towards these enormous information, ordinary PC frameworks are not skillful to store and process these information. Due to the adaptable and flexible figuring assets, distributed computing is a characteristic fit for putting away and handling enormous information. With distributed computing, end-clients store their information into the cloud, and depend on the cloud server to share their information to different clients (information buyers). With a specific end goal to just share end-clients' information to approved clients, it is important to configuration get to control components as indicated by the prerequisites of end-clients. While outsourcing information into the cloud, end-clients lose the physical control of their information. In addition, cloud specialist co-ops are not completely trusted by end-clients, which influences the entrance to control all the more difficult. For instance, if the conventional access control systems (e.g., Access Control Lists) are connected, the cloud server turns into the judge to assess the entrance approach and settle on get to choice. Therefore, end-clients may stress that the cloud server may settle on wrong access choice purposefully or unexpectedly, and reveal their information to some unapproved clients. Keeping in mind the end goal to empower end-clients to control the entrance of their own information, some trait based access control plans are proposed by utilizing characteristic based encryption. In trait based access control, end-clients initially characterize get to approaches for their information and scramble the information under these entrance strategies. Just the clients whose traits can fulfill the entrance strategy are qualified to decode the information.

II. PROBLEM STATEMENT

1. Problem Statement:

As the outsourced data are likely to contain sensitive privacy information they are typically encrypted before uploaded to the cloud. and it is difficult to perform search over encrypted files.

2. Goals & Objectives:

_ Upload file with multikeyword and stored keyword in Encrypted Format
_ File Stored in Encrypted Format using AES Algorithm for Secure File Content

_ Search file by Secret key and Generate Trapdoor
_ File Decryption using Symmetric key.

3. Scope:

In cloud, clients transfer their records on cloud and furthermore get to documents from cloud .So this plan gives an effective encryption plan to security of information put away on cloud and afterward proficient access approach on information documents. Additionally an effective document including with time stamp. Record transferring on cloud with timestamp so it will be available to client just for timestamp related with it. A productive seeking instrument is actualized via looking documents with numerous watchwords and access the cloud information with catchphrase, characteristic and time.

III. PROPOSED SYSTEM

- In Proposed System method can hide the whole attribute (rather than only its values) in the access policies.
- Data Store in Encryption(Cipher Text) and Download in Decryption(Plain Text)
- In this System, we propose an efficient and fine-grained big data access control scheme with privacy-preserving policy. Specifically, we hide the whole attribute (rather than only its values) in the access policies.
- To assist data decryption, we also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

IV. ALGORITHM

1. Advanced Encryption Standard

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

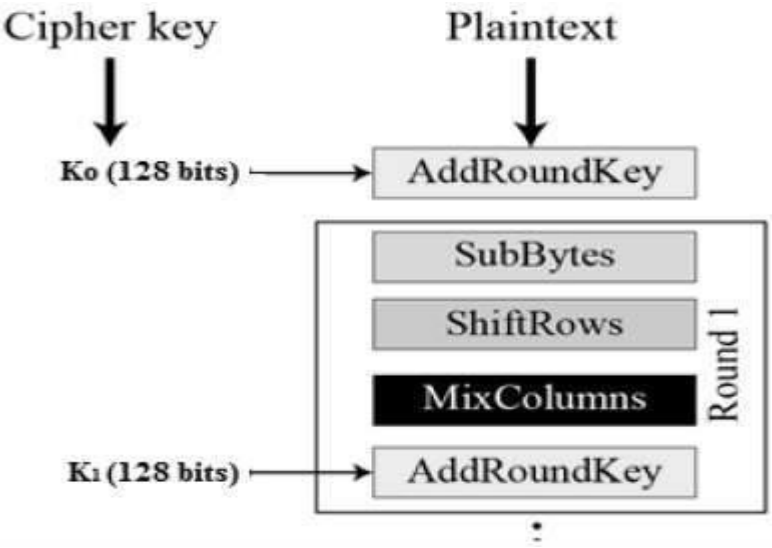
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

A. Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –



1) Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2) Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3) MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4) Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

B. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

A. SYSTEM ARCHITECTURE

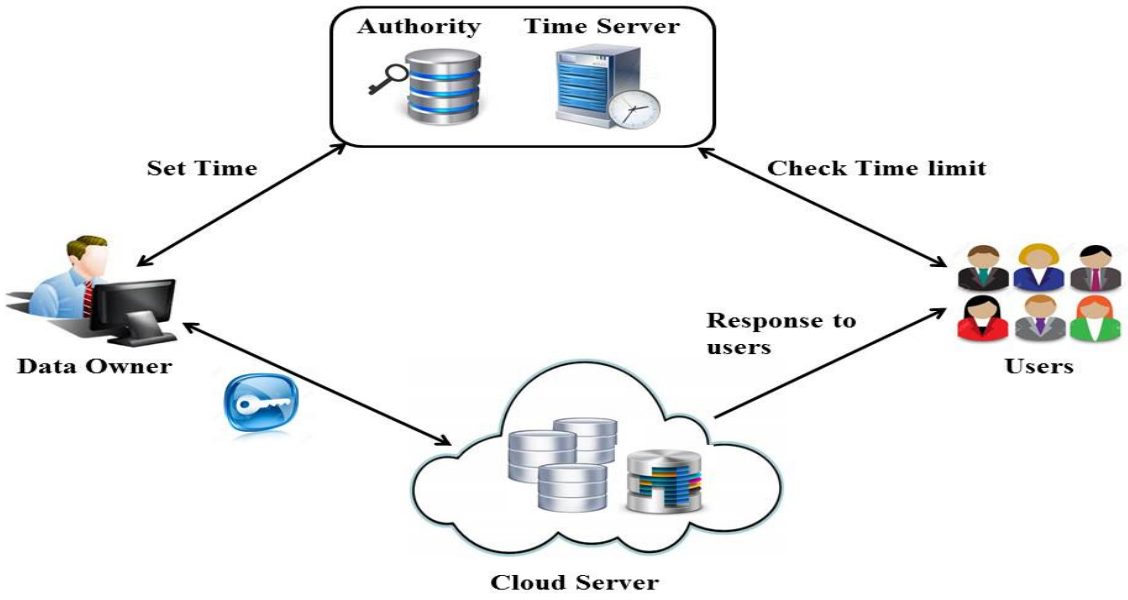


Fig.: System Architecture

B. REQUIREMENTS SOFTWARE AND HARDWARE:

Hardware Requirements Specification:

There should be required devices to interact with software.

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Ram : 256 Mb.

Software Requirements Specification:

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE, Hibernate.
- IDE : Java eclipse.
- Web server : Apache Tomcat 7.

V. APPLICATION

- Medical store applications
- Banking application
- Web Application

VI. RESULT

	(Existing)	(Proposed)
Security	50.6	89.6
Encryption	55.8	91
Accessibility	44.3	98.2
Robustness	80.2	96.09
Accuracy	86.34	99.02

Figs: Result Table

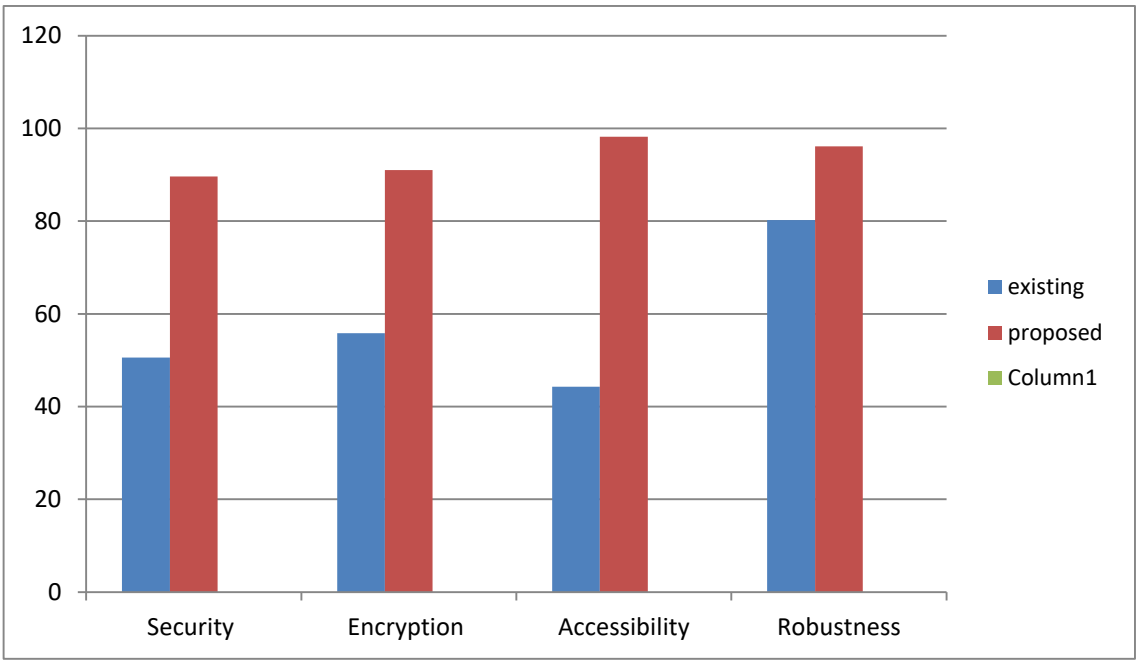


Fig: Time line chart of Result Analysis

VII. CONCLUSION AND FUTURE WORK

We have explored on the fine-grained multi watchword look (FMS) issue over encoded cloud information, and proposed two FMS plans. The FMS I incorporates both the importance scores and the inclination variables of watchwords to upgrade more exact pursuit and better clients encounter, individually. The FMS II accomplishes secure and effective hunt with commonsense usefulness, i.e., AND, OR and NO activities of watchwords. Besides, we have proposed the upgraded plans supporting grouped sub-word references (FMSCS) to enhance proficiency. We mean to additionally stretch out the proposition to consider the extensibility of the record set and the multi-client cloud situations. Towards this bearing, we have made some preparatory outcomes on the extensibility and the multiuser cloud conditions.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, An smdp based service model for inter domain resource allocation in mobile cloud networks, IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 22222232, 2012.
[2] M. M. Mahmoud and X. Shen, A cloud-based scheme for protecting source location privacy against hotspot-locating attack in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 18051818, 2012.
[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, Exploiting geo distributed clouds for e-health monitoring system with minimum service delay and privacy preservation, IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430439, 2014.
[4] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, Privacy preserving data aggregation without secure channel: multivariate polynomial evaluation, in Proceedings of INFOCOM. IEEE, 2013, pp. 26342642.
[5] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, Secure dynamic searchable symmetric encryption with constant document update cost, in Proceedings of GLOBCOM. IEEE, 2014, to appear.
[6] N. Cao, C.Wang, M. Li, K. Ren, andW. Lou, Privacy-preserving multi keyword ranked search over encrypted cloud data, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222233, 2014.
[7] https://support.google.com/websearch/answer/173733?hl=en.
[8] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in Proceedings of S and P. IEEE, 2000, pp. 4455.
[9] R. Li, Z. Xu,W. Kang, K. C. Yow, and C.-Z. Xu, Efficient multi keyword ranked query over encrypted data in cloud computing, Future Generation Computer Systems, vol. 30, pp. 179190, 2014.
[10] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage, IEEE Transactions on Emerging Topics in Computing, 2014, DOI10.1109/TETC.2014.2371239.

