A SURVEY PAPER ON DATA STORAGE SECURITY IN CLOUD COMPUTING

M. Jeevitha
Msc computer science

Dr.M.kannan Assistant Professor [2]
Department of computer science

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE -641 021

ABSTRACT

As Cloud Computing turns into prevalent, greater and greater touchy statistics are being centralized into the cloud. Although common searchable encryption schemes permit a consumer to securely search over encrypted facts via key phrases and selectively retrieve documents of interest, these strategies help solely specific key-word search. In this paper, for the first time we formalize and clear up the trouble of fantastic fuzzy key-word search over encrypted cloud records while retaining key-word privacy. Fuzzy key-word search extensively enhances machine usability with the aid of returning the matching documents when users' looking out inputs precisely suit the predefined key phrases or the closest feasible matching documents primarily based on key-word similarity semantics, when genuine in shape fails. In our solution, we take advantage of edit distance to quantify key phrases similarity and increase two superior strategies on establishing fuzzy key-word sets, which attain optimized storage and illustration overheads. We similarly endorse a manufacturer new symbol-based trie-traverse looking scheme, the place a multi-way tree shape is constructed up the usage of symbols converted from the resulted fuzzy key-word sets. Through rigorous safety analysis, we exhibit that our proposed answer is impenetrable and privacy-preserving, whilst efficaciously realizing the aim of fuzzy key-word search. Extensive experimental outcomes display the effectivity of the proposed solution.

Keywords*: Cloud, Data security, Web based, Java

INTRODUCTION

Cloud computing is an open fashionable mannequin which can allow ubiquitous computing and supply community get admission to to a shared team of configurable computing resources. It gives allotted computing surroundings consisting hardware, software program and services. Apart from this, it presents storage house and help execution of a range of offerings and statistics processing. Cloud protection handles the weak spot and susceptibility of cloud computing. Cloud safety can be labeled as: Cloud Data Security and Storage Security. Data protection ensures the privateness and confidentiality of shared information whilst the storage safety ensures the correctness of the uploaded facts saved in untrustworthy cloud servers. But cloud computing has many challenges involving each information and storage security. While sharing the facts in cloud space, the cloud carrier issuer (CSP) can absolutely gather get admission to to all consumer data. So, information sharing deliver challenges in phrases of protection in cloud computing. The essential privateness and protection necessities of records sharing

Author for correspondence: **M. Jeevitha**

in cloud are: Data Confidentiality and User revocation. Presented a comparative lookup Analysis of the present methods concerning information protection.

Related Work

This simple strategy interestingly presents fuzzy key-word search over the encrypted documents whilst accomplishing search privateness the usage of the approach of impervious trapdoors. However, this strategies serious effectivity disadvantages. The easy enumeration technique in establishing fuzzy key-word units would introduce massive storage complexities, which extensively have an effect on the usability.

For example, the following is the list editions after a substitution operation on the first personality of key-word.

METHODOLOGY

Data Security and purchaser facts privateness are the key challenges in cloud computing era. The appropriateness and privateness of statistics saved in cloud may additionally be compromised due to the fact of constrained protection for information owners. This paper offers an huge survey on privateness preservation, statistics and storage protection difficult problems in cloud computing. The Security of cloud records is similarly analyzed in phrases of statistics integrity, get admission to manage and attribute primarily based encryption. The survey analyzes every class of work in detail. A contrast desk is additionally presented alongside with the energy and weak point of every approach. Other aggregate of algorithms may additionally now not encrypt all sorts of documents such as audio and video which has non-stop bits of facts which may also end result in loss of statistics after encryption, however the proposed machine is strong sufficient to encrypt all sorts of documents except any loss of facts which makes it beneficial for actual time functions.

Problem Statement

Entity Relationship Diagram
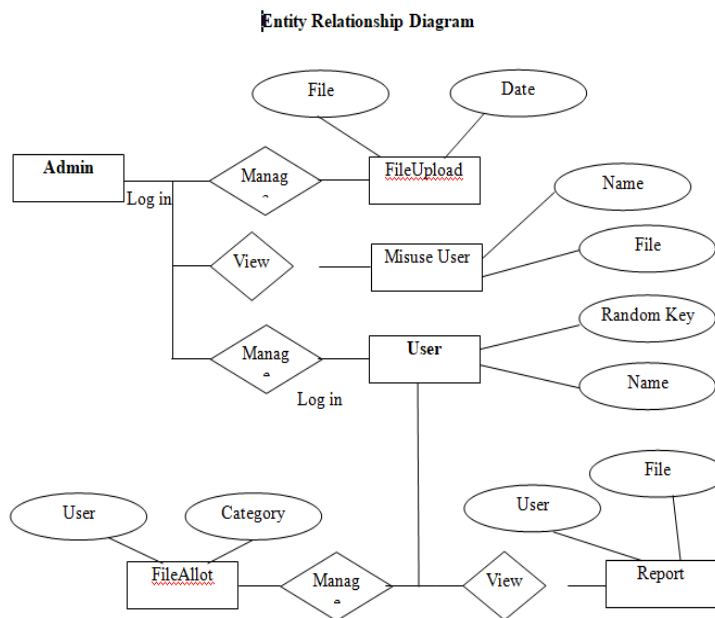
Texture Analysis
1. Outsourcing and Encrypting Data

In the above mention approach we outsource set the data in which fuzzy keyword search techniques must be implemented. The data that is outsourced is encrypted. Hence, security measures are implemented on data stored in cloud server. The encryption technique used her is AES.

2. Wildcard Based Technique

In the above straightforward approach, all the variants of the keywords have to be listed even if an operation is performed at the same position. Based on the above observation, we proposed to use an wildcard to denote edit operations at the same position. The wildcard-based fuzzy set edits distance to solve the problems. For example, for the keyword CASTLE with the pre-set edit distance 1, its wildcard based fuzzy keyword set can be constructed as
Edit Distance

Author for correspondence: M. Jeevitha

a) Insertion Substitution: changing one character to another in a word;

b) Deletion: deleting one character from a word;

c) Insertion: inserting a single character into a word.
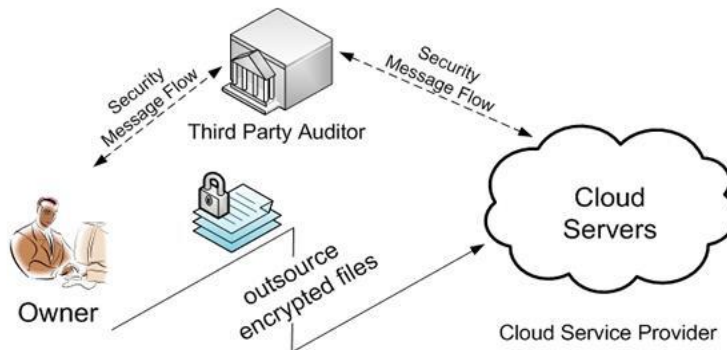
3. Gram Based Technique

Another environment friendly method for setting up fuzzy set is based totally on grams. The gram of a string is a substring that can be used as a signature for environment friendly approximate search. While gram has been broadly used for developing inverted listing for approximate string search, we use gram for the matching purpose. We advocate to make use of the truth that any primitive edit operation will have an effect on at most one unique persona of the keyword, leaving all the last characters untouched. In different words, the relative order of the ultimate characters after the primitive operations is usually stored the equal as it is earlier than the operations. For example, the gram-based fuzzy set SCASTLE, 1 for key-word CASTLE can be developed as {CASTLE, CSTLE, CATLE, CASLE, CASTE, CASTL, ASTLE}.
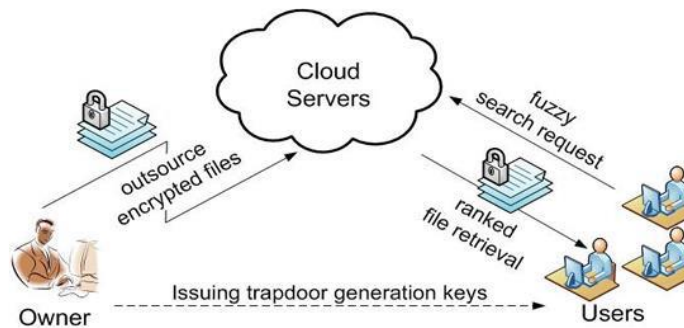

4. Data retrieval

The last end result ie. Data bought from encrypted structure is given to the customers on request. Depending on user's key given by means of the owner, the facts for the unique consumer are viewed. It implies the fuzzy strategies stated above and to decorate the search efficiency, we now suggest a symbol-based trie-traverse search scheme, the place a multi-way tree is developed for storing the fuzzy key-word set over a finite image set. The key thought at the back of this development is that all trapdoors sharing a frequent prefix may also have frequent nodes. The root is related with an empty set and the symbols in a trapdoor can be recovered in a search from the root to the leaf that ends the trapdoor. All fuzzy phrases in the trie can be discovered via a depth-first search.

In this section, we think about a herbal extension from the preceding single-user putting to multi-user setting, the place a records proprietor shops a file series on the cloud server and permits an arbitrary team of customers to search over his file collection.

Author for correspondence: **M. Jeevitha**

Output

Author for correspondence: **M. Jeevitha**
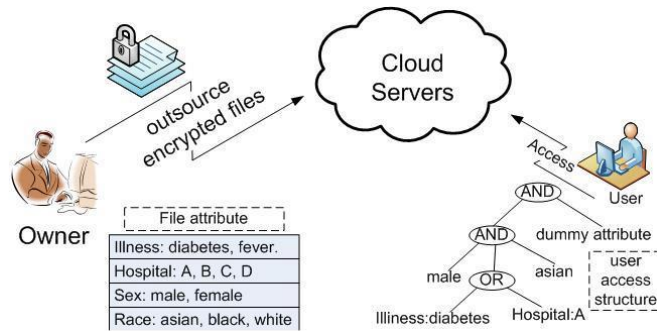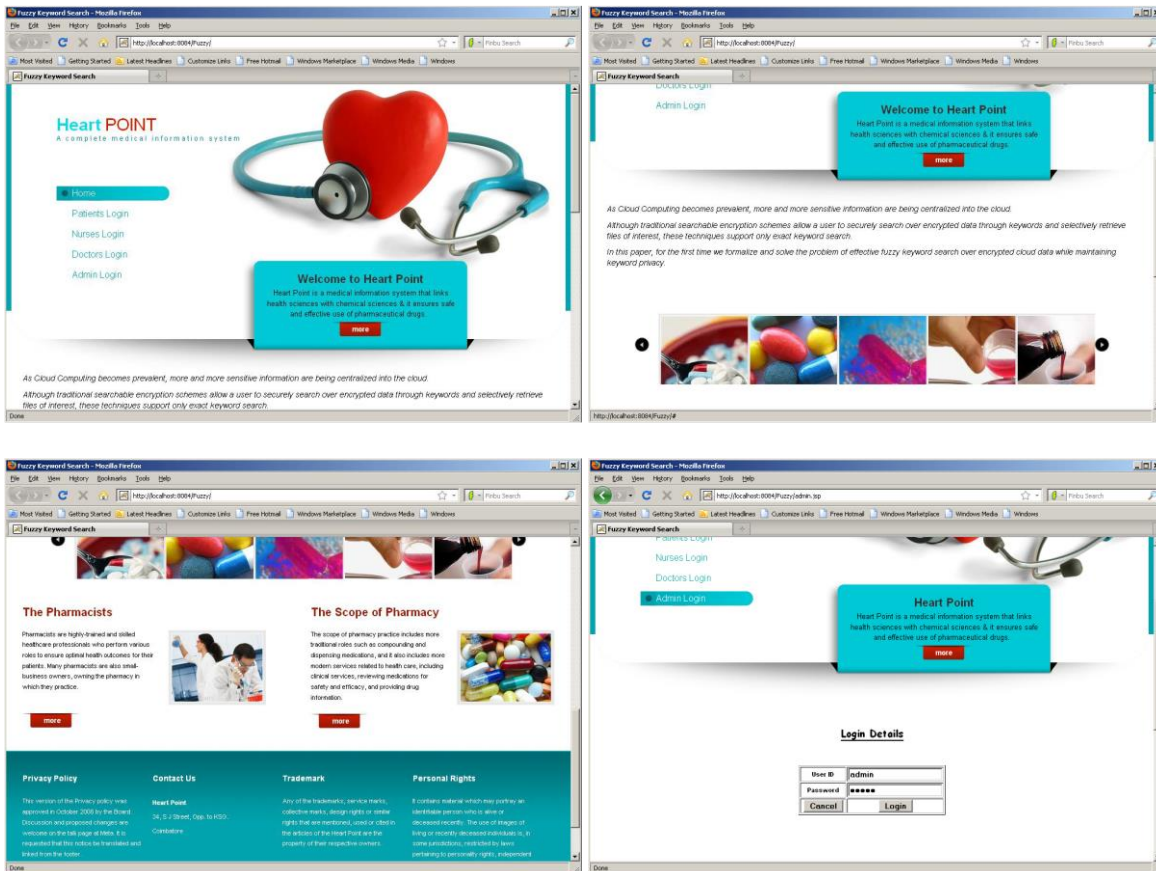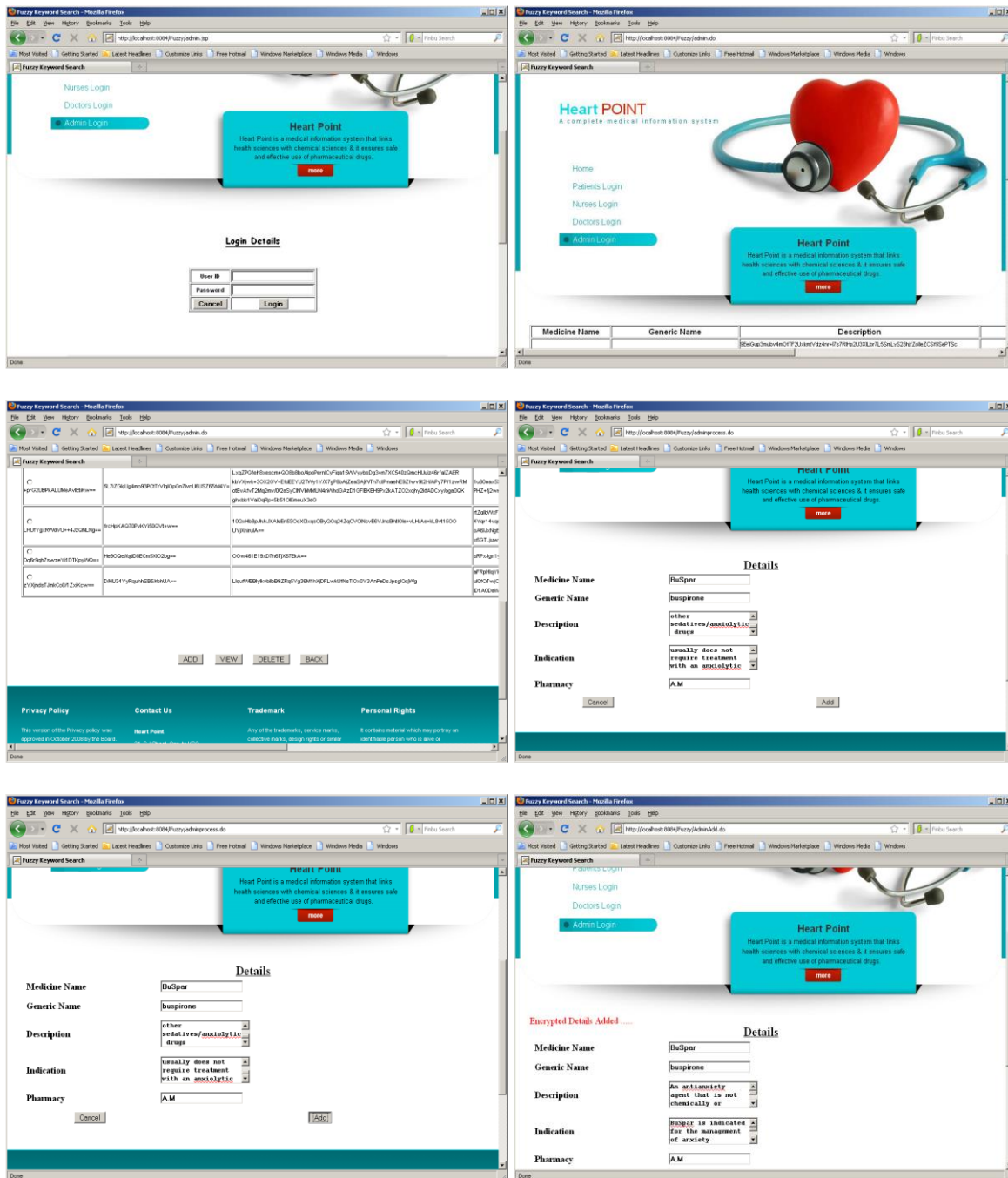
System Testing

The motive of trying out is to find out errors. Testing is the procees of attempting to find out each achievable fault or weak point in a work product. It offers a way to take a look at the performance of components, sub assemblies and/or a completed product. It is the system of exercising software program with the intent of making sure that the Software device meets its necessities and person expectations and does now not fail in an unacceptable manner. There are a number of sorts of test. Each check kind addresses a particular trying out requirement.

Types of Testing
Unit Testing

The developer includes out unit checking out in order to take a look at if the precise module or unit of code is working well. The Unit Testing comes at the

Author for correspondence: M. Jeevitha

very primary stage as it is carried out as and when the unit of the code is developed or a unique performance is built.

Static and Dynamic Analysis

Static evaluation entails going via the code in order to discover out any viable defect in the code. Dynamic evaluation includes executing the code and inspecting the output.

Statement Coverage

In this kind of testing, the code is completed in such a manner that each and every assertion of the utility is finished at least once. It helps in assuring that all the statements execute barring any aspect effect.

Branch Coverage

No software program utility can be written in a non-stop mode of coding. At some factor we want to department out the code in order to function a precise functionality. Branch insurance checking out helps in validating of all the branches in the code and making certain that no branching leads to the peculiar conduct of the application.

Security Testing

Security Testing is carried out in order to discover out how properly the machine can guard itself from unauthorized access, hacking, cracking, any code injury etc. This kind of checking out wants state-of-the-art trying out techniques.

Mutation Testing

It is a sort of checking out in which the utility is examined for the code that used to be modified after fixing a specific bug/defect. It additionally helps in discovering out which code and which method of coding can assist in creating the performance effectively.

Besides all the checking out kinds given above, there are some extra sorts which fall underneath each Black field and White field checking out techniques such as practical checking out (which offers with the code in order to take a look at its useful performance), incremental integration checking out (which offers with the trying out of newly brought code in the application), overall performance and load trying out (which helps in discovering out how the specific code manages sources and supply overall performance etc.) etc.

CONCLUSION

Cloud Computing affords a vary of blessings relative to standard infrastructure Today, it is no longer quintessential to recognize what Cloud gives to the customer, however instead to recognize the hassle of facts protection that is managed through a 0.33 party. This paper addresses the hassle of facts safety in cloud computing. First, we outline information safety issues in three dimensions: cloud characteristics, statistics existence cycle, and information protection attributes. We then described the normal solutions used to guard records for every crew of this classification. In our classification, records safety problems show up to rely on numerous criteria, such as statistics measurement (small /large) statistics kind and identification (persona / personal / use) and facts status(used, saved or transferred). The parameters rely on person Cloud competencies that rely on the kind / provider used in their turns. The privacy, integrity, and available information may additionally be influenced with the aid of these characteristics. We have additionally discovered that the general options used to securing information in the cloud machine are basic techniques for information securing in traditional environments such as encryption and get entry to control. These options are additionally combined and/or cloud-friendly. It is additionally centered on the have confidence the purchaser has in the vendor, as nicely as prison concerns, to preserve facts safety in cloud now not to be summarized as a technological safety solution. Protection and manipulate of IP rights is an vital concern. Cloud Computing facts transfer, collection, and evaluation contain the detection of mental property rights shielding mechanisms for these information.

Future work

In this article, for the first time we formalize and clear up the trouble of aiding environment friendly but privacy-preserving fuzzy search for accomplishing superb utilization of remotely saved encrypted records in Cloud Computing. We layout two advanced strategies (i.e., wildcard-based and gram- based totally techniques) to assemble the storage-efficient fuzzy key-word units via exploiting two widespread observations on the similarity metric of edit distance. Based on the developed fuzzy key-word sets, we similarly advise a manufacturer new symbol-based trie-traverse looking out scheme, the place a multi-way tree shape is constructed up the use of symbols converted from the resulted fuzzy key-word sets. Through rigorous protection analysis, we exhibit that our proposed answer is tightly closed and privacy- preserving, whilst effectively realizing the purpose of fuzzy key-word search. Extensive experimental outcomes display the effectivity of our solution.

Author for correspondence: **M. Jeevitha**

REFERENCES

1. An YZ, Zaaba ZF, Samsudin NF. Reviews on security issues and challenges in cloud computing. IOP Conf S Mater Sci Eng. 2016;160(1):012106. doi: 10.1088/1757-899X/160/1/012106.
2. Arjun U, Vinay S. A short review on data security and privacy issues in cloud computing. In: IEEE International Conference on Current Trends in Advanced Computing. IEEE Publications; 2016. p. 1-5.
3. Balogh Z, Turčáni M. Modeling of data security in cloud computing. In: IEEE annual systems conference. IEEE Publications; 2016. p. 1-6.
4. Bhabad AV, Heda JR, Dhatrak VN, Shahane GP, Shirole BS. Data confidentiality and security in Cloud Computing using KIST algorithm. [Cercle numérique des industries stratégiques (2012)]. Int J Emerg Trends Sci Technol. 2016;1:2456-0006.
5. Charanya R, Aramudhan M. Survey on access control issues in cloud computing. In: IEEE International Conference on Emerging Trends in Engineering, Technology and Science. IEEE Publications; 2016. p. 1-4.
6. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: IEEE International Conference on Computer Science and Electronics Engineering. Vol. 1. IEEE Publications; 2012. p. 647-51.
7. Choubey SD, Namdeo MK. Study of data security and privacy preserving solutions in cloud computing. In: IEEE International Conference on Green Computing and Internet of Things. IEEE Publications; 2015. p. 1101-6.
8. Cyril BR, Kumar SBR. Cloud computing data security issues, challenges, architecture and methods-a survey. Int J Eng Technol. 2015;2:848-57.
9. Delettre C, Boudaoud K, Riveill M. Cloud computing, security and data concealment. In: IEEE Symposium on computers and communications. IEEE Publications; 2011. p. 424-31.
10. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. J Internet Serv Appl. 2013;4(1):5. doi: 10.1186/1869-0238-4-5.
11. Jain P, Gyanchandani M, Khare N. Big data privacy: a technological perspective and review. J Big Data. 2016;3(1):25. doi: 10.1186/s40537-016-0059-y.
12. Kulkarni G, Gambhi J, Patil T, Dongare A. A security aspects in cloud computing. In: International 3rd IEEE 3rd, editor Conference on Software Engineering and Service Science. IEEE Publications; 2012. p. 547-50.
13. Albugmi AA, Alassafi MO, Walters R, Wills G. Data security in cloud computing. In: IEEE Fifth International Conference on Future Generation Communication Technologies. IEEE Publications; 2016. p. 55-9.
14. Lenka SR, Nayak B. Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int J Comput Sci Trends Technol 2. 2014;8578:2347.
15. Mahmood Z. Data location and security issues in cloud computing. In: IEEE International Conference on Emerging Intelligent Data and Web Technologies. IEEE Publications; 2011. p. 49-54.
16. Meng D. Data security in cloud computing. In: IEEE International Conference on Computer Science & Education. IEEE Publications; 2013. p. 810-3.
17. Mohamed EM, Abdelkader HS, El-Etriby S. Enhanced data security model for cloud computing. In: 8th International Conference on Informatics and Systems, p. IEEE Publications. IEEE Publications; 2012. p. CC-12.
18. Munier M, Lalanne V, Ardoy PY, Ricarde M. Métadonnées et aspects juridiques: vie privée vs sécurité de l'information. In: 9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'information; 2014. p. 65-76. SARSSI.
19. Namasudra S, Roy P. Secure and efficient data access control in cloud computing environment: a survey. Multiagent Grid Syst. 2016;12(2):69-90. doi: 10.3233/MGS-160244.
20. Priya Lyer KB, Manisha R, Subhashree R, Vedhavalli K. Analysis of data security in cloud computing. In: IEEE International Conference on Communication and Bio-Informatics Advances in Electrical, Electronics, Information. IEEE Publications; 2016. p. 540-3.

Author for correspondence: M. Jeevitha