Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

Enhancing Privacy of the Content in Web using Random Key Generation Algorithm

Dr. Kumar P
Professor and Head of the Department,
Department of Computer Science and Engineering,
Rajalakshmi Engineering College,
Chennai, India

Anjana K
PG Scholar,
Department of computer Science and Engineering,
Rajalakshmi Engineering College,
Chennai, India.

***Abstract:-* Online websites is an sort of Encyclopaedia which contain millions of articles related to different domains. The major issue found in these websites is the absence of security for numerous files uploaded without any protection thus it is easily available for outside users to edit ,download, or upload the content of these files. Thus to overcome the above drawback we propose the system "Enhancing Privacy Of The Content In Web Using Random Key Generation Algorithm" which makes all the files protected using a individual key generated for each file uploaded in the database were other than the registered user no one can try to access the content. Even the registered user must request to the admin in order to get the key for the particular file they searched for to access it. Thus the system provides an secured data access with originality of the information uploaded bythe data owner, it also avoids the duplication of the same content which is been uploaded many times by same or different users of web.**

I.INTRODUCTION

Nowadays the use of information available in online web such as Wikipedia, Google are evolved in order to mine the details from the available pages in web for the users knowledge. The major flaw in the present system is absence of less security to files stored in database of the websites. In order to resolve we proposed a model "Enhancing Privacy Of The Content In Web Using Random Key Generation Algorithm" were the system protects all the files uploaded in the websites by generating individual keys for each file stored. If any user need to edit or download or upload the information of the content need to register and send request to the admin to get the keys for the file they searched and then they can read or download or update the file content with the permission. We also have a system were the content owner can choose the unwanted words which should not be added in the document at the time of uploading the file so that it reduces the bad debts in the content.

Cloud computing provides the computing power to deal with big data applications on various domain were the data owners are involved to outsource their data with privacy for the content.The most common type of privacy available for large datasets is to encrypt data before outsourcing.The general issue is the query access for encrypted data which is done using index based tree traversal with multikeyword.[1]

The relevancy of data retrieved for the searched keyword issues in major drawback which directly attains in cloud which results in traffic in retrieving unwanted files which is not related to the issues searched.Thus these issues are solved by the searchable secure encryption(SSE) [2]and open secure enryption(OSE)[3] which enhances the search through the encrypted data with the keyword.But the only option for the search is boolean search which consumes much time to get only the related files from the list.

The cloud consist of many primitive and saptial database which are encrypted for privacy.The k-NN is a scheme which is used were the domain of classification, ordering and clustering is involved in the search.The multiple keys for access and privacy of the content are given to both user and data owner which causes and impact of access to content without any rules causes uneven authorisation to files [4][5].

The different keys for a single file causes mapping issues which can cause confusion in the retrieval of the files from the cloud for the users.The mapping function are solved through the index matching and tree based search without giving any access to the key of the file thus by avoiding the unwanted key access to the users of the file and by having an resonable search time for file.The workflow for searching the file using the keyword is one of the issue faced during access of the file .The another main issue is maintaining the key credentials of each file which enhances the security of file[6][7].

The data protection is one of the most vital area of cloud were it acquires an set of techniques followed to protect data.The Data protection is The data protection one of the most vital area of cloud were it acquires an set of techniques followed to protect data which is commonly called as secure socket scheme(SSS) were it includes all sort of protection schemes.The data must be protected for authorised user to access only going through secured access[8][10].

The extraction of the file is also based on extraction algorithm which is been used as iterative and non iterative learning format for searching the files from the database.The system also varies according to the loaction of the information using supervised learning algorithm[11].The system also carries the ranked search through the keywords were the files are arranged according to the keyword which are frequently searched using TF-IDF algorithm.The system also uses encryption for file protection were the access of the file is restricted for the users of web[12][13].

The data available is also handled using iterative graph were the details are summarised through graph with the details of the keyword and content of each file.The system also uses all sort of iterative indexing using the ranking algorithm[14].The effectiveness of the system is also done through the most cited files used by the users of the site.The flow of searching and privacy of the files are maintained through the encryption algorithm available were the key generation is also done through the number generator algorithm for having an idealised content without any unauthorised user to access the file system from cloud without the knowledge of the data owner who actually posted the file to the cloud for outsourcing of the content[15].

II.LITERATURE SURVEY

The cloud security goals include three points as confidentiality, integrity, availability. Encryption is the most common way to secure the data available in cloud. The encryption process includes various deviations were the system handle the data security through key generation algorithms. The encryption algorithm has major division as symmetric algorithm and asymmetric algorithm. It also has various division of graph based algorithm for providing privacy to the content.

The asymmetric key algorithm is used in systems were multiple key is been used for both encryption and decryption of content. The asymmetric key is used in Data Encryption Standard(DES).It is a block cipher which is been used in various encryption phases. It uses an 64bit plain text into 64bit cipher text. The major formation in this algorithm is there are two keys. One key is for encrypting the content and another key for decrypting the content for user access. The key access is made safe so that the authorisation is difficult. But the DES causes many flaws were the key access are cracked.

The flaws of the DES algorithm used in all the above survey issues are overcome by another encryption technique which is symmetric key algorithm which is the Advanced Encryption Standard(AES) algorithm were it deals with single key format. The encryption and decryption are done using the same key with larger key length. The algorithm handles more than 128bits were it is used in large content sets.

The AES algorithm is more secured and cannot be cracked so easily thus the data will be protected without any issue. The algorithm is more efficient for encryption process were the file is protected from unauthorised access without the permission of data owner. Thus from all the above survey issues we have proposed a work to enhance the security of content in web without any changes or offensive action added to the content in web.

III.PROPOSED WORK

Many user centered platforms are available for sharing knowledge with the use of web. The security threats for the contents in web is not secured completely which resulted in unauthorized modifications of the original content without the permission of the data owner who uploaded the content. The main motive of the proposed system is to provide security .

The proposed system uses AES algorithm for encryption process and uses Random Key Generation algorithm for creating keys for each file.The AES algorithm is used for encrypting the file content before it is uploaded in web. This makes the file content unreadable for the users. The security for the content in web is done were the algorithm has larger key length for encrypting the file content.

The another algorithm used in the proposed work is the Random key Generation algorithm which helps the user to select the required key for the file that they upload. This makes the data owner to choose the key for the file which is not available to all the users to access. This system makes the data owner to choose key for the file that they upload in web. This key will be saved with the file details in the database were whenever any user who want to access the file content need to give an request to the admin of the site to get the key for the file to access the content.

The key geneartion algorithm is more secured were no one can guess the next key as it is randomised. This will enhance the security concerns of the content in web and allow only authorised users to acess the file with the request and response for the file. This makes the system more secured and efficient for the users with the original content without any unwanted or offensive changes to the content.

IV.CONCLUSION

Web services have evolved as a flexible and cost effective solution for using the information in web by distributed applications. The web service is the fundamental part of daily life activity were the user depends on the knowledge information given by each website in order to make the user to get more efficient content. However one of the major challenges in web is the security concerns to the content in each websites which are in open access for the user to read and modify the originality of content which leads to collapse and bad debts to the content and the other users. In this proposed system , Random Key Generation and Advance Encryption Standard (AES) is used in order to generate key for each file in web and also use encryption of content that provides high security than the existing security scheme. Thus it provides each user of the site to get the original information without any disruptions.

V.REFERENCES

[1] Xiaofeng Ding, Peng Liu and Hai Jin(2017) “Privacy-Preserving Multi-keyword Top-*k* Similarity Search Over Encrypted Data” IEEE Transactions on Dependable and Secure Computing.

[2] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou(2017) *“*Secure Ranked Keyword Search over Encrypted Cloud Data” IEEE Cloud Computing Service.

[3] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou(2017) “Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data” IEEE Cloud Computing Security.

[4] Ke Cheng, Liangmin Wang,Yulong Shen, Hua Wang, Yongzhi Wang,Xiaohong Jiang, and Hong Zhong (2017)“Secure *k*-NN query on Encrypted Cloud Data with Multiple Keys” IEEE Transaction on Cloud Computing.

[5] Tomoaki Urata, Akira Maeda (2017)“An Entity Disambiguation Approach Based on Wikipedia for Entity Linking in Microblogs” 6th IIAI International Congress on Advanced Applied Informatics.

[6] Jingyun wang, Brendan (2017) “Semi automatic construction on ontology based on data mining technique” 6th IIAI .

[7] Tao jang,Hongzi yu(2017) “Mining Tibetan-Chinese Billingual Language from Wikipedia” IEEE conference.

[8] K.D.C.G. Kapugama, S.A.S. Lorensuhewa, M.A.L. Kalyan(2016) “ Enhancing Wikipedia Search Results Using Text Mining” International Conference on Advances in ICT for Emerging Regions.

[9] Masato Tokuhisa, Yuuki Ishihara, Shuuhei Kimura(2016)“Recommending Paragraphs of Wikipedia Pages as a Travel Guide” IEEE 9th International Workshop on Computational Intelligence and Applications.

[10] KireJakimoski(2016) “Security Techniques for data protection in Cloud” International Journal of Grid and Cloud Computing.

[11] Wengen Li, Jaboe(2016) “Text Rank Algorithm for exploiting Wikipedia for Short text Keyword extraction”3rd International Conference on Information Science.

[12] Muhidin Mohamed(2016) “An Iterative Graph based Generic Single and Multi document summarization Approach using Semantic Role Labeling and Wikipedia Concept” IEEE 2nd International Conference in Big Data.

[13] Keita Tsuji(2016) “Books Citied in Wikipedia”5th IIAI conference in Applied Informatics.

[14] Sruthi v, Surekha Maria(2016) “Secure Multikeyword Retrieval over Encrypted Cloud Data using Harmonic Functions” IOSR Journal of Computer Engineering.