International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 1565-1569
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

EFFICIENT KEYWORD SEARCH OVER HASHED VALUES

Kumara Krishnan[1] ,P SreeramAravind[2], C Velmurugan[3], K S Dhilip[4]
[1]Associate Professor,[2 3 4], Student, B.Tech, CSE, SMVEC, Puducherry.

ABSTRACT: Efficient keywords search is to maintain data's securely without any leakage. To maintain the data's we are protecting them by using the **keywords**, user itself can provide their own keywords related to the file when they are uploading the files. After providing the keywords the keywords will be converted to hash values this is achieved by using hash algorithm once the keywords are have been converted to hash values the keywords will not be in a readable format. The main objective of our project is to use a set off keywords for a confidential file then we need to convert those keywords in to hash values. Our proposed system uploads a file they should be register first and after the registration process they need to login to upload their files while they are uploading their files it will ask for keywords at that time they need to give a set of keywords relevant to the uploading file after finishing certain credentials the keywords will beconverted to hash values, the hash values are achieved using hash algorithm once the keywords are have been changed to hash values the file will be uploaded successfully .Then if they need to download the file in the future means they need to login and enter the keyword in the search box if the setoff keywords matched their requested document means the document will be displayed and if they click the download link means a OTP will be send to their mail-id they need to enter that OTP in the textbox if the OTP matched means the selected file will be downloaded.

INTRODUCTION

Cloud Computing provides us means by which we can access the applications as utilities over the internet. It allows us to create, configure, and customize the business applications.The term Cloud refers Network or Internet. In other words, we can say thatCloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

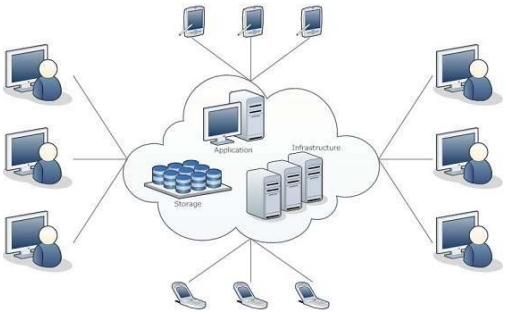


Fig 1. Cloud Computing

1. MODELS IN CLOUD COMPUTING

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing. Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

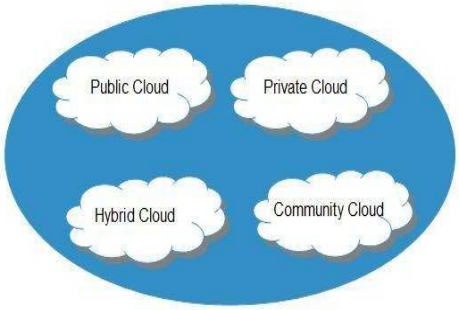


Figure 1: Cloud Computing Deployment Models

Cloud computing [9-10] is based on service models. These are categorized into three basic service models which are Infrastructure-As-A-Service(Iaas)**,** Platform-As-A-Service (Paas)**,** Software-As-A-Service (Saas)**.**

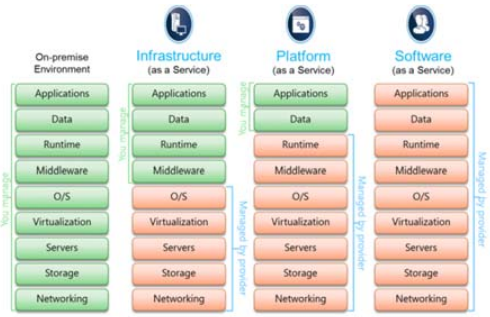


Figure 2: Services in Cloud Computing

Cloud Computing [3-8] has numerous advantages. Some of them are listed below -One can access applications as utilities, over the Internet. One can manipulate and configure the applications online at any time. It does not require to install a software to access or manipulate cloud application. Although cloud Computing is a promising innovation with various benefits in the world of computing, it comes with risks. Some of them are Security and Privacy**,** Lock In**,** Isolation Failure. The characteristics of cloud computing are On Demand Self Service**,** Broad Network Access**,** Resource Pooling

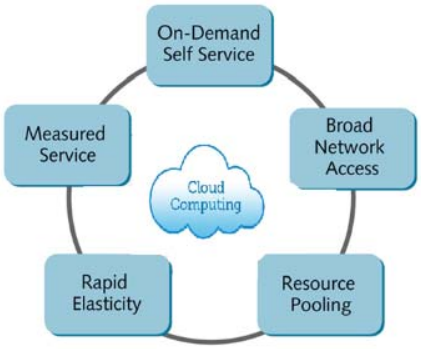


Figure 3: Characteristics of Cloud Computing

2. ANDROID

Introduction:

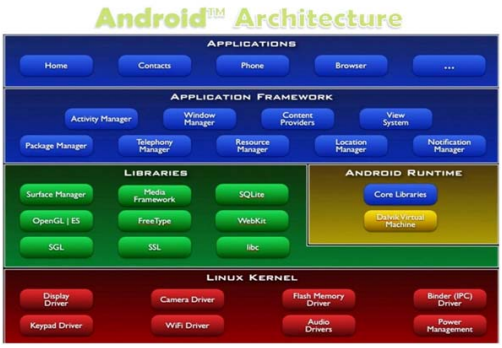
Android is a Linux based operating system it is designed primarily for touch screen mobile devices such as smart phones and tablet computers. The operating system have developed a lot in last 15 years starting from black and white phones to recent smart phones or mini computers. One of the most widely used mobile OS these days is android. The android is software that was founded in Palo Alto of California in 2003.

The android is a powerful operating system and it supports large number of applications in Smartphones. These applications are more comfortable and advanced for the users. The hardware that supports android software is based on ARM architecture platform. The android is an open source operating system means that it's free and any one can use it. The android has got millions of apps available that can help you managing your life one or other way and it is available low cost in market at that reasons android is very popular.

Android Architecture:

The android is a operating system and is a stack of software components which is divided into five sections and four main layers that is

a. Linux kernel
b. Libraries
c. Android runtime



Linux kernel:

The android uses the powerful Linux kernel and it supports wide range of hardware drivers. The kernel is the heart of the operating system that manages input and output requests from software. This provides basic system functionalities like process management, memory management, device management like camera, keypad, display etc the kernel handles all the things.

Libraries:

The on top of a Linux kennel there is a set of libraries including open source web browser such as web kit,

library libc. These libraries are used to play and record audio and video.

Android Runtime:

The android runtime provides a key component called Dalvik Virtual Machine which is a kind of java virtual machine. It is specially designed and optimized for android. The Dalvik VM is the process virtual machine in the android operating system. It is a software that runs apps on android devices.

Application frame work:

The application frame work layer provides many higher level services to applications such as windows manager, view system, package manager, resource manager etc. The application developers are allowed to make use of these services in their application.

Applications and Features:

You will find all the android applications at the top layer and you will write your application and install on this layer. Example of such applications are contacts, books, browsers, services etc. Each application perform a different role in the overall applications.

3. RELATED WORK

PAPER - I Techniques for Efficient Keyword Search in Cloud Computing

In this paper P.Niranjan Reddy and Y.Swetha proposed the following. Cloud computing becomes most general, the important information is centralized into the cloud server. To protect the data stored in the cloud, the data must be encrypted. Although traditional encryption techniques allows the user to securely search through the keyword and return retrieved files, these techniques are useful only for exact keyword search. In this paper, we solve the problem of exact keyword match by providing searching with fuzzy keyword. We also propose two more techniques called gram base technique which is useful for reducing the time, providing fast searching and increase the performance by considering substring from the given string. And Symbol-based tree traverse search scheme where a multi way tree structure is built by using symbols, which works for more than one keywords entered by the user. By providing security, we show that the proposed solution is secure and privacy-preserving.

4. RESEARCH DIRECTION

1. If this algorithm is used, files will be protected**.**
2. In this algorithm, searched keywords file is only visible to the user.
3. In this the verification will be done before downloading the file. So this would be secure.
4. Only particular file will be viewed to the user.

PAPER – II An Efficient Privacy-Preserving Ranked Keyword Search Method:

In this Chi Chen,Xiaojie Zhu, PeisongShen, J.Hu,S.Guo,Z.Tari, and Albert Y. Zomaya, proposed the following. Cloud data owners prefer to outsource documents in an encrypted form for the purpose of privacy preserving.Therefore it is essential to develop efficient and reliable ciphertext search techniques. One challenge is that the relationshipbetween documents will be normally concealed in the process of encryption, which will lead to significant search accuracyperformance degradation. Also the volume of data in data centers has experienced a dramatic growth. This will make it evenmore challenging to design cipher text search schemes that can provide efficient and reliable online information retrieval on large volume of encrypted data. In this paper, a hierarchical clustering method is proposed to support more search semantics andalso to meet the demand for fast ciphertext search within a big data environment. The proposed hierarchical approach clustersthe documents based on the minimum relevance threshold, and then partitions the resulting clusters into sub-clusters until theconstraint on the maximum size of cluster is reached. In the search phase, this approach can reach a linear computationalcomplexity against an exponential size increase of document collection. In order to verify the authenticity of search results, astructure called minimum hash sub-tree is designed in this paper. Experiments have been conducted using the collection setbuilt from the IEEE Xplore. The results show that with a sharp increase of documents in the dataset the search time of theproposed method increases linearly.

whereas the search time of the traditional method increases exponentially.Furthermore, theproposed method has an advantage over the traditional method in the rank privacy and relevance of retrieved documents.

5. CONCLUSION

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public-key setting, cryptographic primitive called

public-key encryption with keyword search (PEKS). This focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Also, we proved it's a security in the standard model, and analyzed its efficiency using computer simulations.

6. FUTURE ENHANCEMENT

In cloud server ,we propose encrypted data in the public key encryption with keyword search has produced efficient cryptographic public key setting. we proposed the computation time of searching a document rangers from 50sec to 2.50sec for a trapdoor with 10 keywords and a cipher text with 50keywords . In future, the computation time can be significantly reduced.

REFERENCE

[1] P. Niranjan Reddy et al, "Techniques for Efficient Keyword Search in Cloud Computing" International Journal of Computer Science and Information Technologies, Vol 4 No.1, 2013, 66 - 68

[2] Chi Chen, Xiaojie Zhu, PeisongShen, J.Hu, S.Guo, Z.Tari, and Albert Y. Zomaya, "An efficient privacy-preserving ranked keyword search method", IEEE Transactions on Parallel and Distributed Systems January 2015,DOI:10.1109/TPDS.2015.

[3] Vigneshwaran, R., Janakiram, A., Jarina, S., Prem Kumar, K., Anantharaj, B., Sathian, D., "An empirical analysis on Quality of Service(QoS) in cloud computing", (2016) Indian Journal of Science and Technology, 9 (22), art. no. 95181,

[4] Karthikeyan, P., Sathian, D., Raghav, R.S., Abraham, A., Dhavachelvan, P., "A comprehensive survey on variants and its extensions of BIG DATA in cloud environment", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743097,

[5] Padmapriya, V., Bakkiya, K., Sujitha, B., Thamizhselvi, M., Premkumar, K., "A scalable service oriented consistency model for cloud environment (SSOCM)", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743089,

[6] Ilamathi, R., Moganarangan, N., Ravishankar, V., Baskaran, R., Premkumar, K., "Performance analysis in cloud auditing: An analysis of the state-of-the-art", (2015) International Journal of Applied Engineering Research, 10 (3), pp. 2043-2046.

[7] Kathavate, P., Reddy, L.S.S., Satyanarayana, K.V.V., "Effects, challenges, opportunities and analysis on security based cloud resource virtualization", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 12), pp. 1458-1463.

[8] Garikapati, G., Yakobu, D., Nitta, G.R., "An analysis of cloud data security issues and mechanisms", (2017) International Journal of Pure and Applied Mathematics, 116 (6 Special Issue), pp. 141-147.

[9] Ramya, U., Reddy, B.T., Sekhara Rao, M.V.P.C., "Enhanced check sum approach for secure deduplication file system in integrated cloud system", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 6), pp. 322-334.

[10] Sandhya, A., Harshini, T., Vyshnavi, T., Vurukonda, N., Rao, B.T., "Scalable attribute based encryption scheme for accessing cloud data", (2017) International Journal of Pure and Applied Mathematics, 115 (8 Special Issue), pp. 541-546.