Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 812-820, April-June 2018

A Distributed Mobile Cloud Computing for Secure Mobile Data

Anand T M[1] and Thiruvenkatasuresh M P[2]

[1]*PG Student, Department of Computer Science and Engineering, Excel Engineering College, Komarapalayam, India .*
[2]*Assistant Professor, Department of Computer Science and Engineering, Excel Engineering College, Komarapalayam, India.*

Article Received: 01 March 2018 *Article Accepted: 09 April 2018* *Article Published: 28 April 2018*

ABSTRACT

A cloud system is difficult to synchronize login and authentication data between external clouds and internal systems without exposing internal security data. The cloud technologies are rapidly being adopted throughout the Information Technology (IT) due to their various attractive properties. In spite of their spread, they have raised a range of significant security and privacy concerns which interrupt their adoption in sensitive environments. In existing scheme makes a good tradeoff between the functionality and the efficiency. To better express the relevance between the query and files, we introduce the TF-IDF rule into our design.

Keywords: Mobile cloud computing, self-proxy server, key manager, distributed cloud computing, mobile cloud provider.

1. INTRODUCTION

Cloud computing is internet-based computing in which large groups of remote servers are networked to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources. Clouds can be classified as public, private or hybrid. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. The main enabling technology for cloud computing is virtualization.

Virtualization software allows a physical computing device to be electronically separated into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. Cloud computing adopts concepts from Service oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way. An individual or an organization may not require purchasing the needed storage devices.

Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. Preserving authorized restrictions on information access and disclosure. The main there at accomplished when storing the data with the cloud. Guarding against improper information modification or destruction and ensuring timely and reliable access to and use of information.

mous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity Wireless sensor network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to

cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance.

2. BACKGROUND AND RELATED WORK

In this paper, a solution is to apply a distributed self proxy re encryption technique, propose a Proxy Server (PS). It coordinates and chooses keys by Key Manager (KM) whenever group membership changes. The distributed SPS provides not only encryption and decryption keys but also immediate re encryption keys for shared data. After communicating with KM, it automatically receives necessary keys from KM by self created algorithm. A distributed SPS scheme is one solution where multiple proxies are automatically deployed in several clouds. In this Module, the cloud service provider can able to login with their provided credentials and can able to View Application Service Provider Details, View Data Owner Details. In this module the Payment from Data Owner will be performed. The details includes of the payments are Cloud storage provider id, data owner id, date of payment, file details and the payment amount.

2.1. Cloud Data Owner

Data The Data Owner (DO) has data to be stored in the cloud and rely on the cloud for data computation, consists of both individual consumers and organizations. The data owner of MCP shares data to many other cloud users. The data is encrypted with a key from KM and then stored in the cloud along with access control list indicating the user group. Upon access request from a user, the cloud communicates with SPS, based on access control list, and Self Proxy Server (SPS) requests for the key.

According to the key request to the SPS, uses re-encryption to transfer the encrypted format that can be decrypted by the user's private key. The user can download the encrypted data from the cloud and use the decryption key. In this data owner module, the data owner can View the Application service provider Details, View CSP Details after logged into the system.

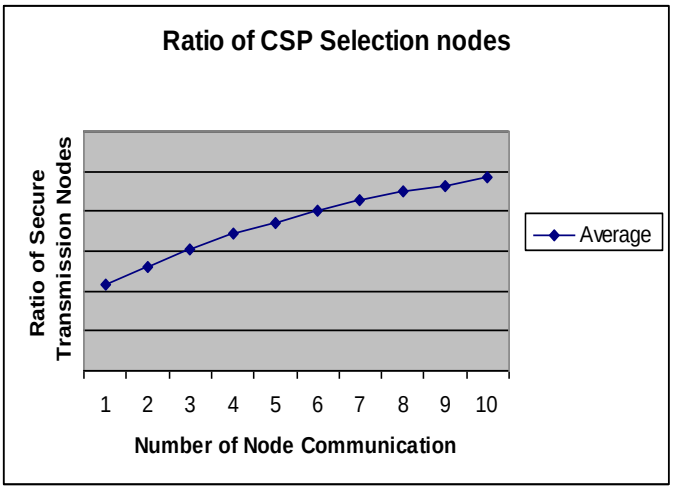
The data owner can also Upload Content to the cloud storage with the description of file description, category of the file and cloud storage provider details along with application service provider details. The data owner can also View the Download Request from the users and Provide Keys to the download request files by the end users.

2.2. Infrastructure with cloud services

The existing system has provided comprehensive information regarding the cloud security problems. It has been estimated the security problem from cloud architecture point of view, the cloud stakeholders' point of view and at the end from cloud services delivery models point of view. From stakeholder prospective, the security

configurations need to be organized and each service should be maintained a level at runtime. From service delivery model prospective, the cloud management security issues and cloud access method security issues are also highlighted.

The existing system has presented details about the security issues which cloud service providers are facing when they dig deep for cloud engineering. There are some serious issues and challenges which cloud computing are facing in the domain of cyber security. The paper also covers security management models for the cloud service providers in order to meet security compliance. The existing system has identified the serious threats and risks related to privacy and security for the mass and corporate users when they will integrate their mobile hand held devices with the cloud infrastructure.



3. PERFORMANCE ANALYSIS

The following Table 7.1 describes experimental result for existing system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of CSP details are shown:

S.NO	NUMBER OF TIME SLOT (M)	RATIO OF SELECTION CSP
1	10	0.43
2	20	0.52
3	40	0.61
4	60	0.69
5	80	0.74
6	100	0.80

7	120	0.86
8	140	0.90
9	150	0.93
10	160	0.97

3.1. Mechanism of existing system

Input central keywords with certain adjunct words as the query keywords when searching documents. The importance of each query keyword depends on the search intension of a user. So far many works have demonstrated the importance of keywords. The super-increasing sequence is to show the preference factors of keywords to indicate the importance of keywords in a query keyword set.

However, users need to sort keywords according to their importance, which increases the users' input cost. Due to the lack of the super-increasing sequence, the last keyword the user inputs are more important than all the other keywords. The existing model built a user interest model for individual user by analyzing his search history.

However, when inputting unusual keywords, it needs to re-build a new interest model. In this project, our use the grammatical relations as standards to show the weight of each keyword, and this enables users to retrieve relevant documents from the cloud based on their own interests.

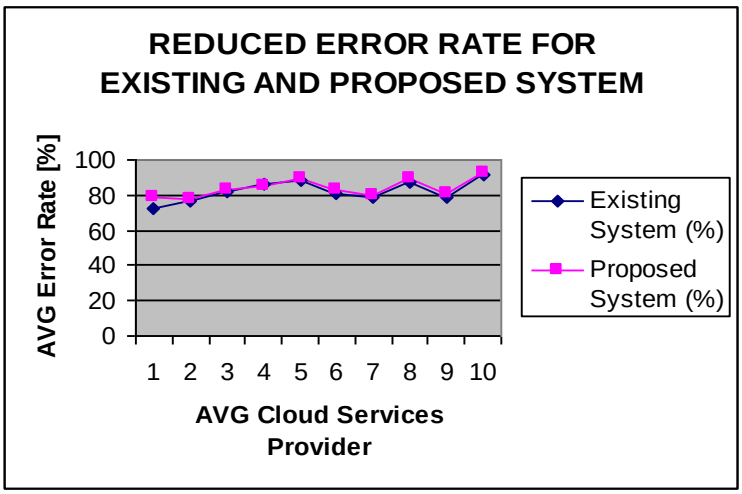
In addition with all the existing system mechanism, a correlated Authentication aspect with combination of the cloud storage provider, application service provider and end user is also considered. In addition, time limit is provided to end user to access the Application Service Providers (ASPs). So at different time intervals, different kinds of tariffs can be applied to end users to access the service. Likewise, the security aspects provided by the cloud storage provider is also taken by ASPs to increase the security more. In addition, trusted third party authentication mechanism is included.

3.2. Term Frequency Analysis

Each Term Frequency – Inverse Document Frequency (TF-IDF)

The TF measures how frequently a particular term occurs in a document. It is calculated by the number of times a word appears in a document divided by the total number of words in that document. It is computed as TF(the) = (Number of times term the 'the' appears in a document) / (Total number of terms in the document). The IDF measures the importance of a term. It is calculated by the number of documents in the text database divided by the number of documents where a specific term appears. While computing TF, all the terms are considered equally important. That means, TF counts the term frequency for normal words like "is", "a", "what", etc. Thus we need to know the frequent terms while scaling up the rare ones, by computing the following: IDF(the) = log_e(Total number of documents / Number of documents with term 'the' in it).

For example, Consider a document containing 1000 words, wherein the word give appears 50 times. The TF for give is then (50 / 1000) = 0.05. Now, assume that, 10 million documents and the word give appears in 1000 of these. Then, the IDF is calculated as log(10,000,000 / 1,000) = 4. The TF-IDF weight is the product of these quantities − 0.05 × 4 = 0.20.

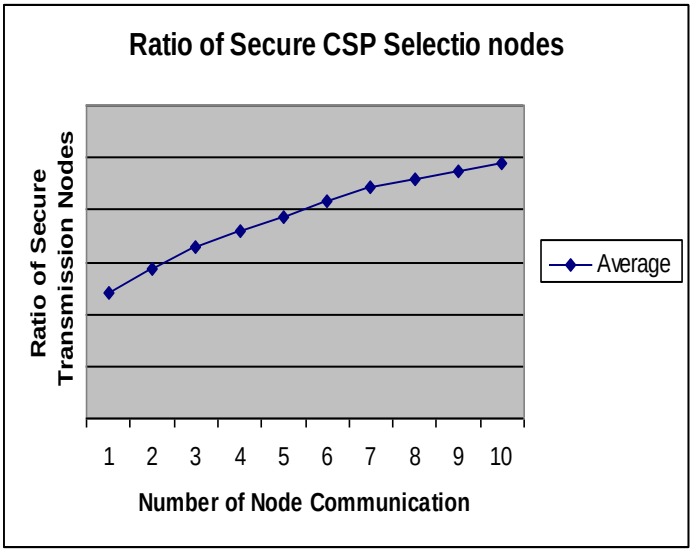


REDUCED ERROR RATE FOR EXISTING AND PROPOSED SYSTEM

Member Node	Existing System (%)	Proposed System (%)
8	72.54	78.62
12	76.13	78.11
16	82.42	83.13
24	86.66	84.67
30	88.13	89.78
32	80.44	82.66
38	78.33	80.21
42	87.22	89.76
46	79.22	80.65
50	91.22	92..62

3.3. End user Search

In this process, the end user search the data can able to view the Cloud Storage Provider Details, Application Service Provider Details and Data Owner Details. The user can also Search for Content from the cloud storage and they can download the file by means of send request to the data owner to obtain the key to download the contents. The user can download the encrypted data from the cloud and use the decryption key.



The following Table 7.2 describes experimental result for proposed system secure transmission node analysis. The table contains number of time slot interval and given time interval to calculate average numbers of send transmission node details are shown:

S.NO	NUMBER OF TIME SLOT (M)	RATIO OF CSP NODE
1	10	0.48
2	20	0.57
3	40	0.66
4	60	0.72
5	80	0.77
6	100	0.83
7	120	0.89
8	140	0.92
9	150	0.95
10	160	0.98

Selection Multi Cloud Services Provider- Ratio Analysis

3.4. Application Service Providers

Input central keywords with certain adjunct words as the query keywords when searching documents. The importance of each query keyword depends on the search intension of a user. So far many works have demonstrated the importance of keywords. The super-increasing sequence is to show the preference factors of keywords to indicate the importance of keywords in a query keyword set.

However, users need to sort keywords according to their importance, which increases the users' input cost. Due to the lack of the super-increasing sequence, the last keyword the user inputs are more important than all the other keywords. The existing model built a user interest model for individual user by analyzing his search history.
However, when inputting unusual keywords, it needs to re-build a new interest model. In this project, our use the grammatical relations as standards to show the weight of each keyword, and this enables users to retrieve relevant documents from the cloud based on their own interests.

In addition with all the existing system mechanism, a correlated Authentication aspect with combination of the cloud storage provider, application service provider and end user is also considered. In addition, time limit is provided to end user to access the Application Service Providers (ASPs). So at different time intervals, different kinds of tariffs can be applied to end users to access the service. Likewise, the security aspects provided by the cloud storage provider is also taken by ASPs to increase the security more. In addition, trusted third party authentication mechanism is included.

3.5. Cloud Service Provider Mechanism

In this process, the admin user can able to add the cloud service provider details, application provider details and data owner details, the details which are stored into the corresponding tables in the data base

Cloud Service Provider details includes the Cloud service provider id, name of the cloud provider, website and password details will be stored into the CSProviders table. Application Service Provider details includes the Application service provider id, name of the application service provider, password are stored into the ASProviders table. Data Owner details includes the data owner id, name of the data owner and password details are stored into the DataOwner table.
Also the admin user assigns the Cloud Service Provider to Application Service Provider and Assign Cloud Service Provider to Data Owner. And the admin user can able to view the Cloud Service Providers details, Application Service Providers details, Data Owners Details; View Users details and view downloads

4. CONCLUSIONS

In this experimental study, the existing system is describing the problem of secure authentication for storage in cloud. In this paper, proposed FA which carries out a flexible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The security analysis

shows that our N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality, integrity and secure access control. Novel-Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes. It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. This work mainly addresses the reading authorization issue on cloud storage. And it results to enable the TPA to perform audits for multiple users simultaneously and efficiently

REFERENCES

[1] Tassanaviboon and G. Gong, "OAuth and ABE based authorization in semi-trusted cloud computing," in Proc. 2nd Int. Workshop Data Intensive Comput. Clouds, 2011, pp. 41–50.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[3] Agudo, "Cryptography goes to the cloud," in Proc. Workshop Secure Trust Comput., Data Manage. Appl., 2011, pp. 190–197.

[4] J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient clientside deduplication of encrypted data in cloud storage," in Proc.8th ACM SIGSAC Symp. Inf., Comput. Commun. Security, 2013, pp. 195–206.

[5] Wang, S. S. Chow, Q.Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans.Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[6] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau,"Dynamic audit services for outsourced storages in clouds," IEEE Trans. Serv. Comput., vol. 6, no. 2, pp. 227–238, Apr.–Jun. 2013.

[7] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011

[8] T. O. Eiichiro Fujisaki, "Secure integration of asymmetric and symmetric encryption schemes," J. Cryptol., vol. 26, no. 1, pp. 80–101, 2013.

[9] Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, Jun. 2007.

[10] R. Berlekamp and L. R. Welch, "Error correction for algebraic block codes," U.S. Patent US 4 633 470 A, Sep. 27, 1983.

[11] Gorenstein, W.W. Peterson, and N. Zierler, "Two-error correcting Bose-Chaudhuri codes are quasi-perfect," Inf. Control, vol. 3, no. 3, pp. 291–294, 1960.

[12] Reed and G. Solomon, "Polynomial codes over certain finite fields," J. Soc. Ind. Appl. Math., vol. 8, no. 2, pp. 300–304, 1960.

[13] L. R. Welch. (1997). The original view of reed-solomon codes [Online]. Available: http://csi.usc.edu/PDF/RSoriginal.pdf

[14] M. Backes, C. Cachin, and A. Oprea, "Secure key-updating for lazy revocation," in Proc. 11th Eur. Conf. Res. Comput. Security, 2006, pp. 327–346.

[15] C. J. Mifsud, "Algorithm 154: Combination in lexicographical order," Commun. ACM, vol. 6, no. 3, p. 103, 1963.

[16] Y.-C. Chen, E. M. Nahum, R. J. Gibbens, D. Towsley, and Y. Lim,"Characterizing 4G and 3G networks: Supporting mobility with multi-path TCP," Univ. Massachusetts Amherst, Amherst, MA,USA, Tech. Rep. UM-CS-2012-022, 2012.

[17] Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.