International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Integrated Approach for Providing Data Security and Integrity over Encrypted Cloud Data

Jami Rama Satya Nookalu [#1], Somayajula Yamini Anupama [#2], Koilada Bharathi[#3] ,Mrs. J.Santoshi Kumari [#4]

[#1,#2,#3] B.Tech Student, Department of CSE ,
Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam, Visakhapatnam, AP, India
[#4] Assistant Professor, Department of CSE ,
Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam, Visakhapatnam, AP, India.

ABSTRACT

In current days cloud domain gained a tremendous increase of user's attention by several small and large scale companies including software, BPO, healthcare, schools, colleges and a lot more. All these organizations try to adopt this centralized cloud server for their data storage and accessing from the remote locations connected all together from a centralized server with the help of internet. All the data is stored remotely and retrieved from the remote machines not from the local machines, hence the secrecy of data plays a vital role by the cloud service providers. As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and message digest in order to provide data authorization. Almost all companies try to search the data in a secure manner over encrypted cloud data, which will allow an untrusted user to query data files of interest by submitting encrypted keywords as a search query to the cloud server. In general, the returned query results may be some times correct or incorrect or incomplete in this dishonest cloud environment. As we all know that in current days cloud servers are almost dishonest in nature by omitting intentionally some qualified results to save computational resources and communication overhead. In this paper, we proposed and analyzed a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the quality of each data file but also checks the total number of qualified data files, which are not returned if the set is not completed before decryption process. This mainly motivated us to design a novel secure verification object for the encrypted cloud storage. Here we also used a message digest algorithm MD5 in which the short signature key is generated and used for verifying the data authentication. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient.

Key Words: Message Digest, Encryption, Decryption, Data Authorization, Privacy, Message Digest.

1. Introduction

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

In recent days cloud computing is one among the several domain for storing the data remotely in unknown machines which users do not own .Even though cloud domain attained a lot of users interest in storing and accessing the data to and from the server, it still face some problem in maintain the data in a secure way. Currently there are lot of service providers who are giving cloud service for personal and enterprise usage like Yahoo, Siliconhouse.net, Amazon, Google, Microsoft,Drivehq and sales force. Hence by using these services users try to enjoy the benefits of data storage and accessing from the remote machines rather than concentrating on the acknowledgement of that remote machines[1].As the data is stored on remote servers, no user is concentrated with authentication of their sensitive data whether valid users are accessing this information or any un-authorized users try to access this data [2].

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Figure. 1. Represents the Various CSP's For Remote Data Storage and Access

From the above figure 1, we can clearly find out various cloud service providers who try to give facility of storing and accessing the data remote manner rather than from the local machines. As we all know that each and every service provider try to provide the main facility like try to store the user data based on their individual request and also try to provide a wide range of storage options based on the individual request. As many of them are showing their interest over cloud storage but still there is a problem like data is stored in the normal way or in the form of plain text without any encrypted manner. So as the data which is uploaded in the cloud is not stored in our own PC rather than it will be stored in a remote PC, there is no level of achieving data integrity in the current cloud service providers. This mainly motivated me to design and develop a novel facility like encryption of data before it is stored into the cloud server and restricting un-authorized users not to access this server. And also for a real time experience drivehq service provider is taken as back end storage cloud for storing the encrypted data into the cloud[3]-[5].

2. Background Work

In this section we will try to study and analyze about the background work that is carried out in designing this fine-grained query results verification over encrypted cloud data. Here we try to analyze about the primitives of cloud computing and their working functionality.

Motivation

Basically **for** any CSP or data hosting service, they are mainly 3 entities like:

1. Data Owner Entity,
2. Cloud Server Entity and
3. Data User/Search User Entity.

Now let us discuss about each and every entity in detail and a small working functionality about those three.

Initially the data owner is one who may be an individual or sometimes an enterprise, who try to outsource a set of valuable or sensitive documents P = (P1, P2, . . . , Pn) in a plain text format and once

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

these documents are uploaded into the server, the server then try to encrypt those plain documents into encrypted manner and those are represented with form E = (E1, E2, . . . , En) to the cloud server. Here we can see all the documents are labeled with a letter 'P' and if there are multiple documents to be uploaded into the server, we distinguish them with letters like P1,P2….Pn.Here the input documents are very sensitive and can be either medical related, salary related, company annual records,shares,employees welfare information and so on. Once the sensitive documents are encrypted and then ready to store inside the cloud server, they are termed as E1, E2 and so as they were encrypted by the data owner at his level before out sourcing into the cloud server[6]-[8].

The next main entity in cloud computing domain is the cloud server, which has the capability to accept, store and provide access permissions for the end users in a secure manner. Initailly the cloud data owner try to encrypt the data and upload those encrypted files into the cloud server,this cloud server will then check the index of documents and arrange all those documents in a indexed manner to avoid redundancy. This cloud server has the facility to view and access the information on its own and even it can change the content from that original files. This is the main reason why we designed our current thesis, in which the admin even try to modify the original content; it can be identified by both end users and data owners. As this is not there in the current cloud servers, all the valuable information is misused at the server end[9].

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

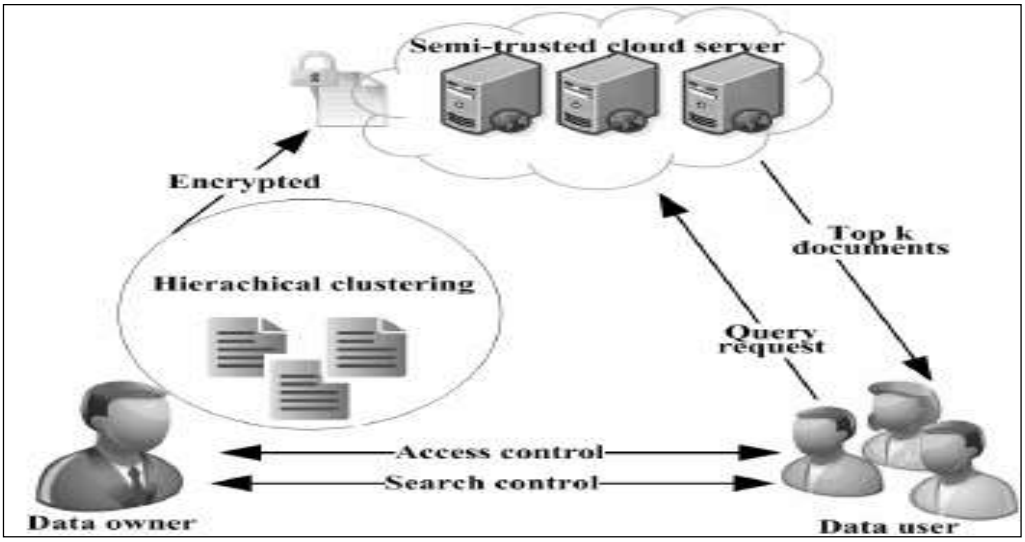

Figure. 2. Represents the Basic Cloud Entities

The final entity in cloud data storage is the end user or search user who wishes to download the files from the cloud server by giving valid inputs for searching the files and then download those files in a secure manner. This entity has mainly 3steps to be performed for downloading the Encrypted documents from the cloud server[10].

Step 1: Initially if the search user wants to download the data from the cloud server, he needs to register into the application and get approval from the cloud admin.

Step 2: Once the end user is registered and got login approval from the cloud admin, then he/she need to enter his valid login credentials and then try to enter into their account. Once they enter into his/her account, the search user need to enter the valid encrypted search keyword in order to download the data from the cloud server.

Step 3: In this step, the cloud user send valid request for file download from his account and this will be reached to the data owner who uploaded that documents into the cloud server. Here the cloud owner is one who is having total permissions to allow or ignore the file download access by the end user. If he allow the access key, the search user can access the file in a plain text

manner. If not the search user cant able to access the file in a plain text manner.

From the above figure 2, we can clearly find out the basic entities of cloud computing domain in which the cloud server is named as semi trusted cloud server, because it is not providing total privacy of data in terms of authorization. Here the data owners are one who try to upload a set of sensitive documents by encrypting them in to the server space and once the data users are registered and login into their account and try to search the documents with a query request keyword. Once if the credentials are matched he can get access control from the owner and decryption keys are send to the end users mail id.If not the users are identified as trapdoor users and they can't access the file.

3. Proposed Integrated Approach for Providing Data Security and Data Integrity

In this section, we mainly describe the proposed unique query results verification scheme for secure data storage and access under MAC algorithm for generating short signature to verify the data correctness.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

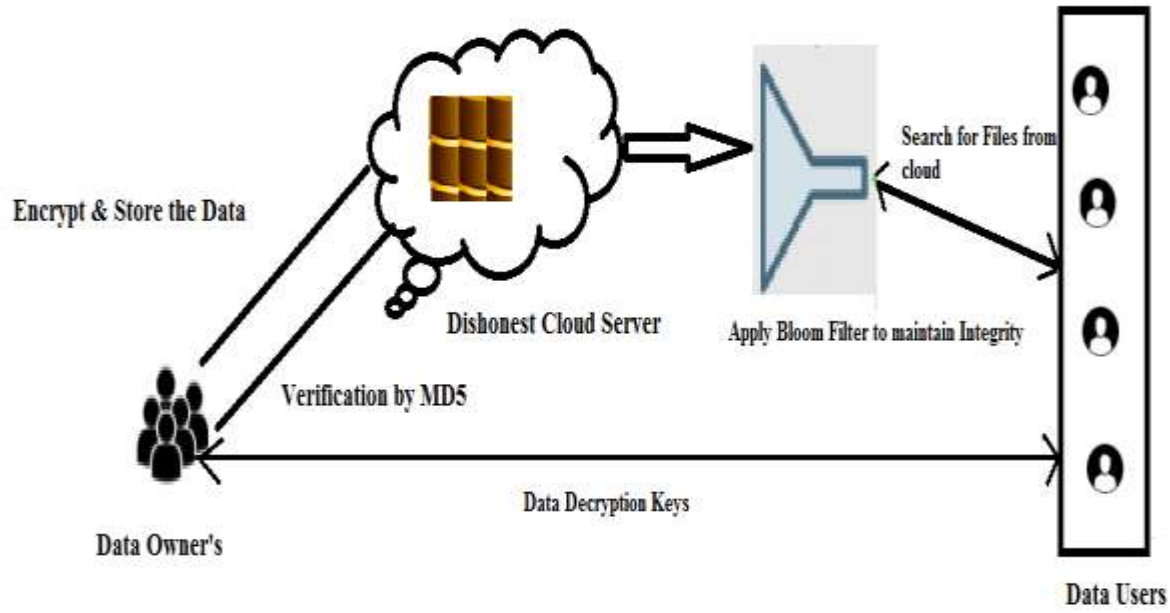

Figure. 3. Represents the Proposed Model For Secure Data Verification Search

From the above figure 3, we can clearly represent the proposed architecture flow diagram of our current thesis which will mainly discuss about the dishonest cloud server and its sub entities that try to store and access data remotely. Initially the data owners try to upload their sensitive files into the cloud server in an encrypted manner. So at once many owners may upload the files from remote locations into the dishonest cloud server. So it is very important to maintain indexes before the file is stored into the server. Once the files are arranged in an index manner, now the data or search users try to extract the required documents from the dishonest cloud server. Now different end users try to request various files from remote locations and all file requests will be received by the data owners and those who are eligible for data download can access the files in a plain text manner and all other cant able to get decryption keys from the data owners[11]. Here this plays a vital role in providing privacy for the sensitive data.

Here in our proposed approach we try to use Bloom Filter for data filtering in which the bloom filter try to provide filter mechanism for the impure data to be filtered

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

at the system level. If there is any data which is modified or injected with any virus the bloom filter will create a backup for the original data and try to filter the data according to that originality content. If the original content and the data which is been extracted by the receiver has any change in the content then the bloom filter will be automatically invoked and the data will be identified as modified and this will be filtered at the system level and the bloom filter will provide a filtered result for the end users.

4. Experimental Result

The proposed application is designed and developed with java programming language, in which the front end of the application is done with HTML, JSP and CSS.The back end of the application is designed with MY-SQL database and for the live storage of data in a secure manner, we try to use a hybrid cloud server like DRIVEHQ.Now the proposed application is verified on some sensitive documents and now let us look about them in detail as follows:

Data User/Search User try to Verify and then download the Sensitive Documents

From the above screen we can clearly identify that the data user try to enter

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

the trapdoor key which is send to the registered mail id and once if the key is correct then it will accept the user request.

From the above window we can clearly identify both the hash key or short signatures are same, so that the decryption key is allowed by the system .If the end user enter the valid decryption key which is received to his mail id, then the data can be decrypted into plain text and can be viewed by the search user.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Now the decryption key is substituted by the data user and now the data can be viewed in a plain text manner.

From the above window we can clearly identify that as both hash keys are same, the data can be decrypted and viewed by the end user, if the user submit download button.

If both has keys are not matched by the search user for the file download, then that file will not have decrypt facility and the file will be always remains in encrypted manner inside the cloud.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

5. Conclusion

In this paper we finally have implemented a we propose a secure, easily integrated, and a novel fine-grained query results verification scheme over encrypted cloud data. Compared with all primitive algorithms, our proposed scheme can accurately verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. In order to attain the principle of authorization a short signature to guarantee the effectiveness of verification object. By conducting various experiments on our proposed model we finally came to an conclusion that this is the first time to implement such a novel method into the cloud for providing privacy and data integrity for the sensitive data which is to be stored into the cloud in a secure manner

6. References

[1] W. Zhang, S.Xiao, Y. Lin, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Transactions on Computers, vol. 65, no. 5, pp.1566–1577, May 2016.

[2] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, 2014.

[3] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,"IEEE Transactions on Parallel and Distributed System, vol. 27, no. 2,pp. 340–352, 2015.

[4] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[5] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. *J. Cryptology*,22(1):1–61, 2009.

[6] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan. Sedic: privacyaware data intensive computing on hybrid clouds. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS'11, pages 515–526, New York, NY, USA, 2011. ACM

[7] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. *J. Cryptology*,22(1):1–61, 2009.

[8] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan. Sedic: privacyaware data intensive computing on hybrid clouds. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS'11, pages 515–526, New York, NY, USA, 2011. ACM

[9] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp. 190–200, 2015.

[10] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

7 .About the Authors

JAMI RAMA SATYA NOOKALU is currently pursuing his 4 Years B.Tech in Department of Computer Science and Engineering, at Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam ,Visakhapatnam, AP, India. His area of interest includes Web Designing and Development.

SOMAYAJULA YAMINI ANUPAMA is currently pursuing her 4 Years B.Tech in Department of Computer Science and Engineering, at Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam ,Visakhapatnam, AP, India. Her area of interest includes Data Analysis.

KOILADA BHARATHI is currently pursuing her 4 Years B.Tech in Department of Computer Science and Engineering, at Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam ,Visakhapatnam, AP, India. Her area of interest includes Web Designing and Development.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Mrs. J.SANTOSHI KUMARI is currently working as Assistant Professor in Department of Computer Science and Engineering, at Nadimpalli Satyanarayana Raju Institute of Technology, Sontyam ,Visakhapatnam, AP, India. She has more than 10 years of teaching experience in engineering colleges. Her area of interest includes Data Mining.