Query Results Verification for Secure Search Scheme over Encrypted Cloud Data

[1]K.Kavya, [2]K.Hareesh Kumar, [3]J.J.Jhansi, [4]D.Harish, [5]G.Anil Kumar

B.Tech. Final Year Students,
Computer Science & Engineering,
MTIET, Palamaner, India

***Abstract*— At ease search strategies over encrypted cloud data permit a certified user to query records files of hobby through filing encrypted query keywords to the cloud server in a privacy-keeping manner. But, in exercise, the again question consequences can be wrong or incomplete in the cheating cloud surroundings. For instance, the cloud server may deliberately pass over a few certified consequences to keep computational sources and conversation overhead. Thus, a properly-functioning comfortable question system has to provide a question outcomes verification mechanism that permits the statistics person to verify effects. In this paper, we layout a comfy, without problems included, and best-grained question effects verification mechanism, by way of which, given an encrypted query outcomes set, the query user now not only can affirm the correctness of every records file inside the set however also can similarly take a look at what number of or which qualified facts documents aren't returned if the set is incomplete before decryption. The verification scheme is free-coupling to concrete cozy search strategies and may be very without difficulty included into any comfy query scheme. We obtain the aim by way of building comfy verification item for encrypted cloud records. Moreover, a brief signature approach with extraordinarily small garage fee is proposed to guarantee the authenticity of verification object and a verification item request technique is supplied to allow the question user to soundly gain the desired verification object. Performance evaluation shows that the proposed schemes are practical.**

***Index Terms*: - Cloud Computing, Verification Object, Query Results Verification, Secure Search Scheme.**

I. INTRODUCTION

Encryption on private facts before outsourcing is an effective degree to shield records confidentiality. However, encrypted records make powerful statistics retrieval a very hard undertaking. To deal with the assignment (i.e., seek on encrypted Information), music et al. First added the idea of searchable encryption and proposed a sensible method that permits customers to go looking over encrypted statistics through encrypted question key phrases in. Later, many searchable encryption schemes had been proposed based totally on symmetric key and public-key placing to reinforce safety and improve question efficiency. Lately, with the growing recognition of cloud computing, the way to securely and efficiently seek over encrypted cloud records will become a studies focus. A few tactics had been proposed primarily based on conventional searchable encryption schemes in which goal to defend statistics protection and question privacies with higher query green for cloud computing. But, all of these schemes are based totally on a really perfect assumption that the cloud server is an ”sincere-however-curious” entity and maintains strong and relaxed software/hardware environments. As a result, accurate and entire question outcomes usually be unexceptionally lower back from the cloud server while a question ends each time. But, in sensible applications, the cloud server may additionally go back inaccurate or incomplete question consequences once he behaves dishonestly for unlawful income inclusive of saving Computation and communication value or due to feasible software program/hardware failure of the server.

II. RELATED WORK

These days, with the growing recognition of cloud computing, a way to securely and efficiently search over encrypted cloud statistics turns into a studies awareness. Some techniques have been proposed based on conventional searchable encryption schemes, which aim to protect records protection and question privacies with higher question green for cloud computing.

- Wang et al. Carried out hash chain technique to put into effect the completeness verification of question outcomes by using embedding the encrypted verification records into their proposed cozy searchable index.
- Sun et al. Used encrypted index tree shape to enforce comfy query outcomes verification functionality. On this scheme, when the question ends, the cloud server returns question consequences at the side of a minimal encrypted index tree, then the information consumer searches this minimal index tree the usage of the same search algorithm because the cloud server did to finish result verification.
- Zheng et al. Constructed a verifiable comfortable query scheme over encrypted cloud facts primarily based on Attribute-Based Encryption technique (ABE) inside the public-key setting.
- Sun et al. Cited the merkle hash tree and applied pairing operations to put into effect the correctness and completeness verification of question consequences for keyword seek over huge dynamic encrypted cloud facts.

DRAWBACKS OF EXISTING SYSTEM:

- Encrypted records make powerful information retrieval a completely difficult undertaking.
- All of these schemes are based on a super assumption that the cloud server is an ”sincere-but-curious” entity and keeps strong and comfy software program/hardware environments. As a result, correct and complete question results always be unexceptionally lower back from the cloud server whilst a question ends each time.
- Those verification mechanisms offer a rough grained verification, i.e., if the question end result set includes all qualified and accurate facts files, then those schemes reply sure, otherwise respond no. Therefore, if the verification set of rules outputs no, a data person has to abort the decryption for all question effects despite only one question end result is inaccurate.
- Those verification mechanisms are normally tightly coupled to corresponding cozy query buildings and feature not universality.

PROPOSED SYSTEM:

In the system, we expand and brief up our paintings to make it more relevant within the cloud environment and greater relaxed to against cheating cloud server. The primary contributions of this paper are we officially suggest the verifiable secure seek gadget version and chance model and design a fine grained query results verification scheme for at ease key-word seek over encrypted cloud information .We advise a quick signature method primarily based on certificate much less public-key cryptography to assure the authenticity of the verification objects themselves. We design a unique verification object request technique based on hashing algorithm, where in the cloud server knows nothing about what the facts person is inquiring for and which verification items are returned to the user.

Advantages of Proposed data:

The following are the advantages of proposed system by overcoming the drawbacks of existing system. These are as follows,

1. We offer the formal protection definition and proof and behavior great performance experiments to evaluate the accuracy and efficiency of our proposed scheme.
2. Our scheme can verify the correctness of each encrypted query result or in addition correctly discover how many or which certified information documents are back via the cheating cloud server.
3. A quick signature approach is designed to assure the authenticity of verification object itself.

SYSTEM ARCHITECTURE:

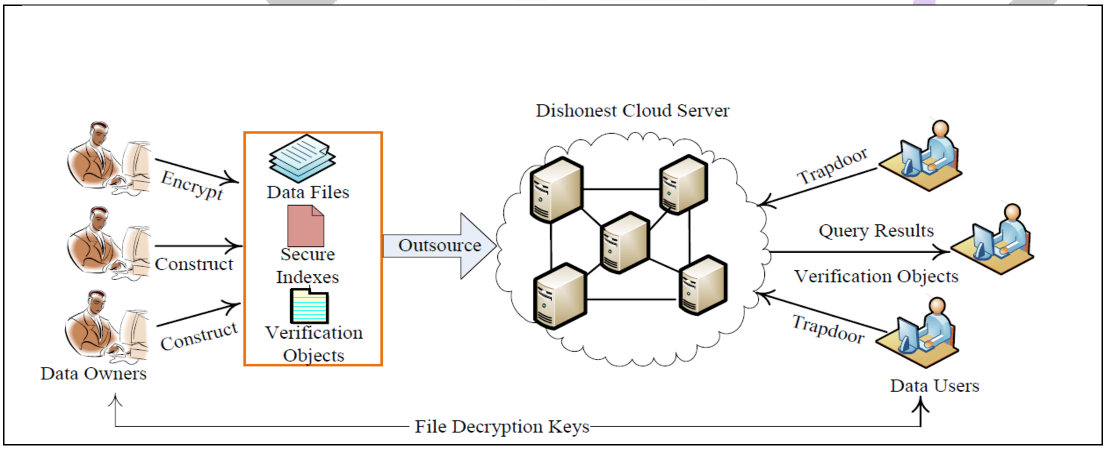


Fig: Query Results Verification in Dishonest Cloud Server

III IMPLEMENTATION

MODULES:

The main modules present in this paper are as follows, these plays major roles in this system.

1. Data Owner
2. Data User
3. Cloud Server

1. Data Owner:

In Data Owner module, Initially Data Owner must have to register their detail. After successful registration data owner can login and upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the trapdoor key and verification object through mail.

2. ***Data User:***

   In Data User module, Initially Data Users must have to register their detail and after login he/she has to verify their login through secret key. Data Users can search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive trapdoor, verification object and decryption key in registered mail

3. ***Cloud Server*:**

   In Cloud Server module, Cloud Provider can view all files details. Cloud can edit the files and update and also cloud server can view the download history.

ALGORITHMS USED:

1. ***AES Algorithm*:**

   AES algorithm is used for encryption of data files uploaded in cloud server by data owner. The same algorithm is used for decryption by the data user while downloading the file from the Cloud Server. The following figure illustrates the process of encryption and decryption.

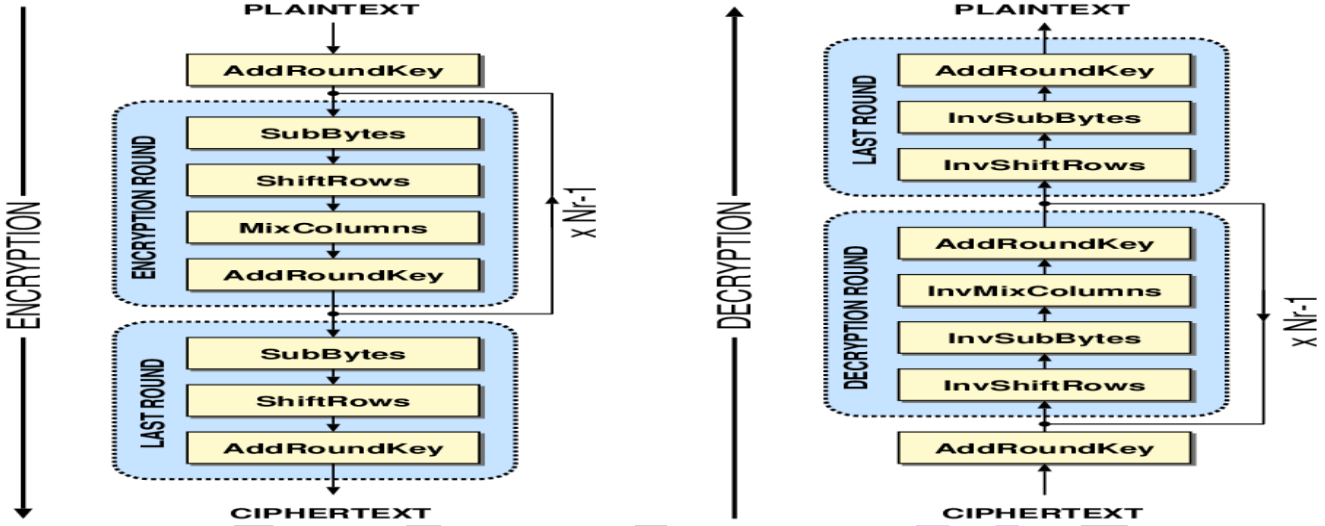


Fig3.1: AES algorithm for Encryption and Decryption

2. ***Hash Algorithm*:**

   Hash algorithm is used to construct the verification object. The following figure illustrates the process involved in hash algorithm.

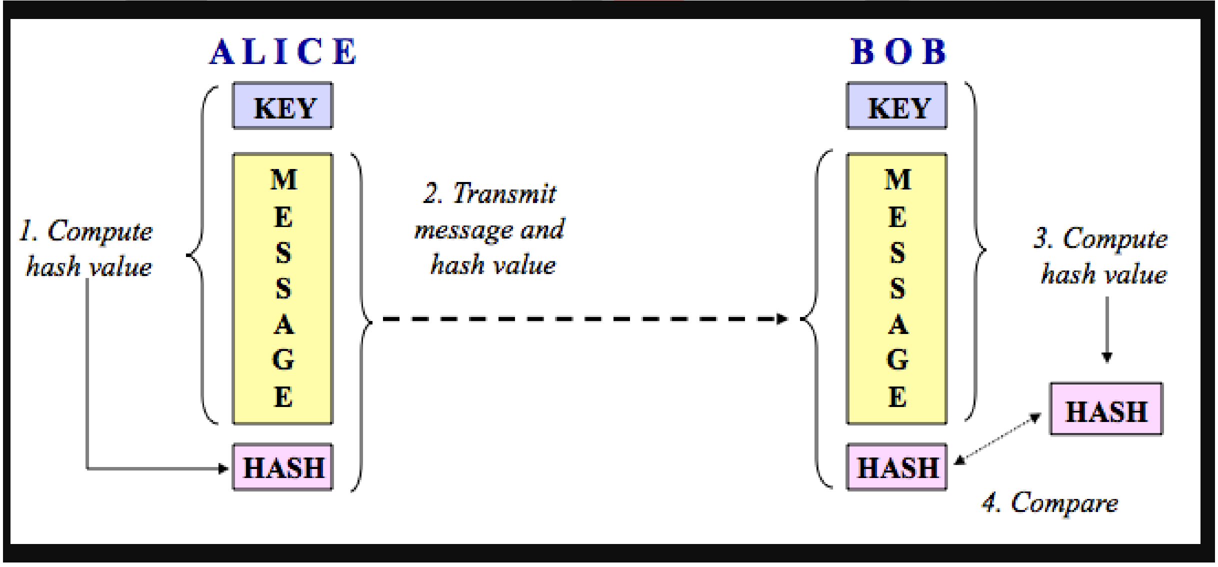


Fig3.2: Process Involved in Hash Algorithm

‘

IV. RESULTS

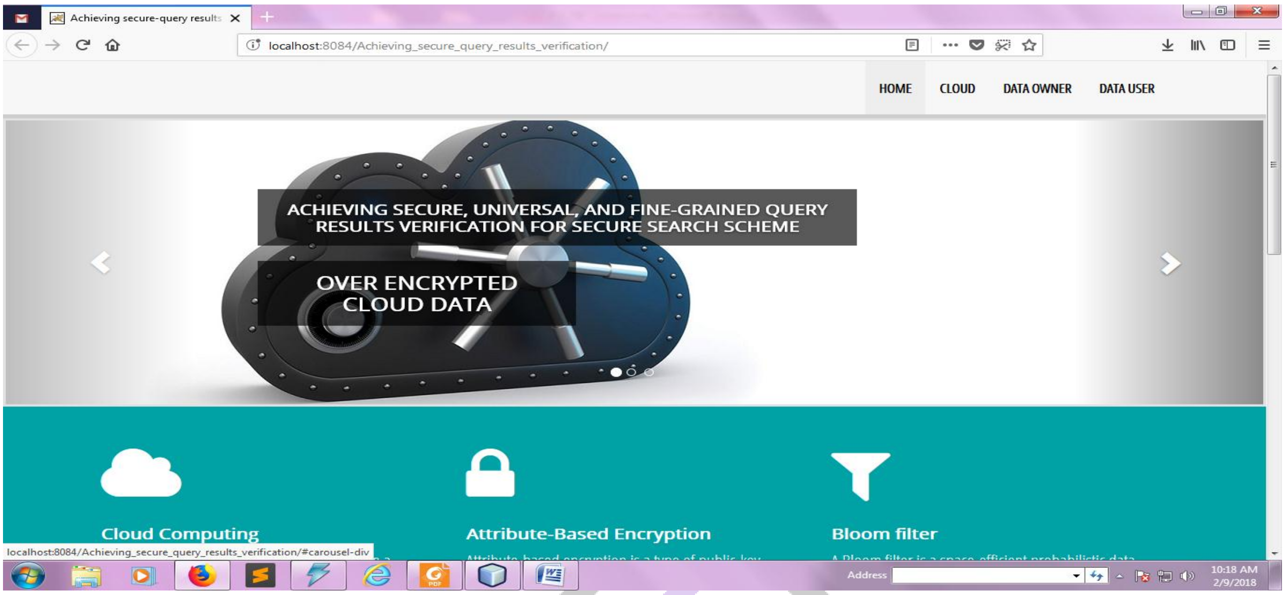

Achieving secure-query results
localhost:8084/Achieving_secure_query_results_verification/
HOME
CLOUD
DATA OWNER
DATA USER
ACHIEVING SECURE, UNIVERSAL, AND FINE-GRAINED QUERY RESULTS VERIFICATION FOR SECURE SEARCH SCHEME
OVER ENCRYPTED CLOUD DATA
Cloud Computing
Attribute-Based Encryption
Bloom filter
localhost:8084/Achieving_secure_query_results_verification/#carousel-div
Address
10:18 AM
2/9/2018

Fig4.1: Cloud Home Page

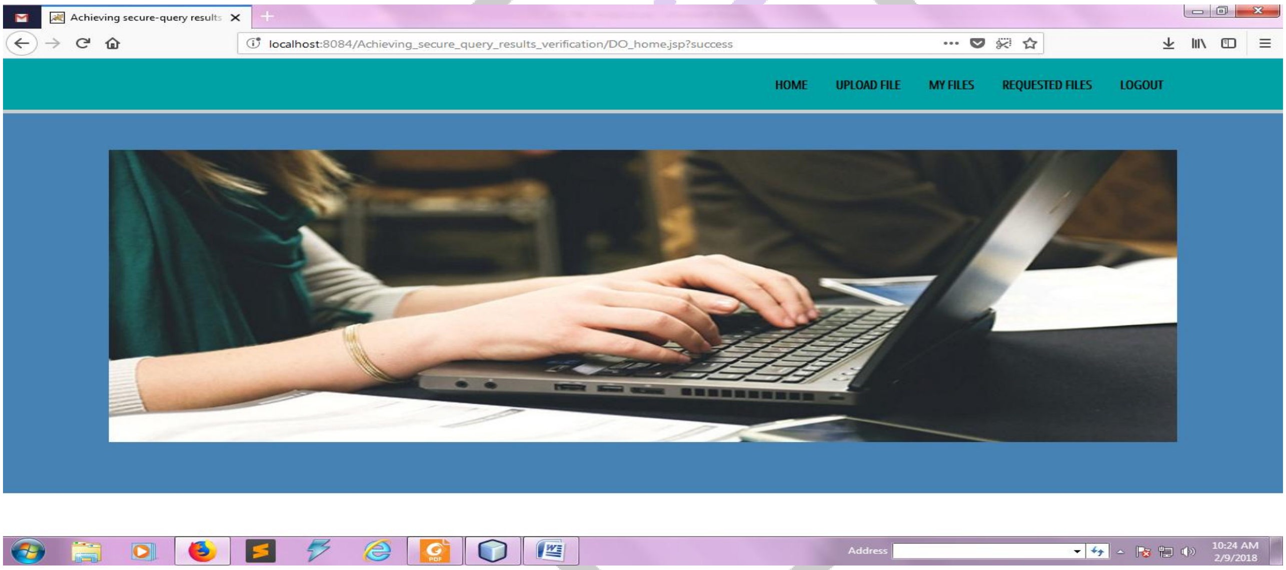

Achieving secure-query results
localhost:8084/Achieving_secure_query_results_verification/DO_home.jsp?success
HOME
UPLOAD FILE
MY FILES
REQUESTED FILES
LOGOUT
Address
10:24 AM
2/9/2018

Fig4.2: Data Owner Home Page

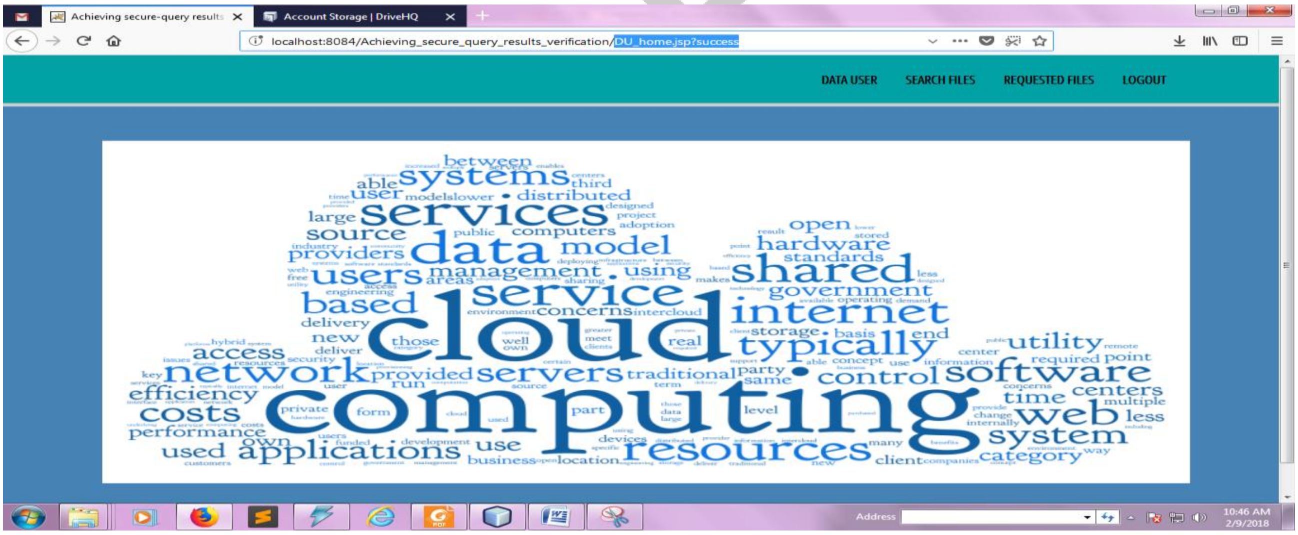
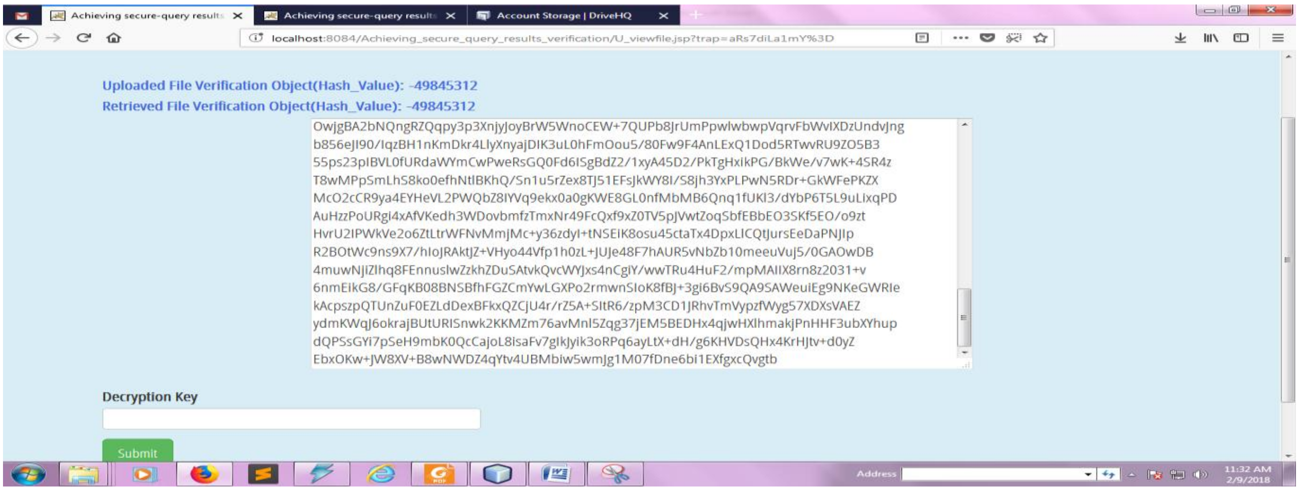


Fig4.3:DataUser Home Page


Achieving secure-query results
Achieving secure-query results
Account Storage | DriveHQ
localhost:8084/Achieving_secure_query_results_verification/U_viewfile.jsp?trap=aRs7diLa1mY%3D
Address
11:32 AM
2/9/2018

Uploaded File Verification Object(Hash_Value): -49845312

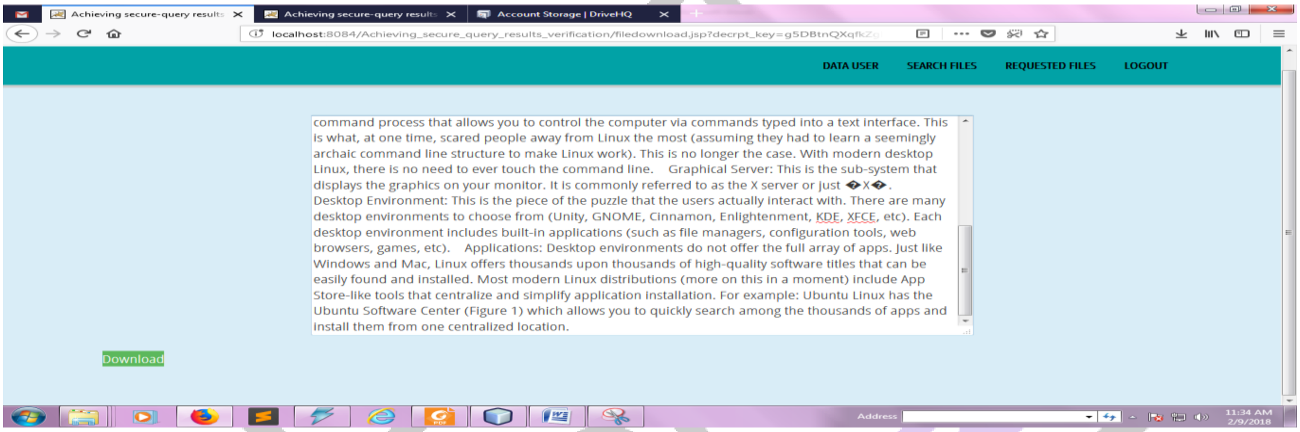
Retrieved File Verification Object(Hash_Value): -49845312

```
OwjgBA2bNQngRZQqpy3p3XnjyJoyBrW5WnoCEW+7QUPb8JrUmPpwlwbwpVqrvFbWvIXDzUndvJng
b856eJI90/IqzBH1nKmDkr4LlyXnyajDIK3uL0hFmOou5/80Fw9F4AnLExQ1Dod5RTwvRU9ZO5B3
55ps23pIBVL0fURdaWYmCwPweRsGQ0Fd6ISgBdZ2/1xyA45D2/PkTgHxikPG/BkWe/v7wK+4SR4z
T8wMPpSmLhS8ko0efhNtlBKhQ/Sn1u5rZex8TJ51EFsJkWY8I/S8jh3YxPLPwN5RDr+GkWFePKZX
McO2cCR9ya4EYHeVL2PWQbZ8IYVq9ekx0a0gKWE8GL0nfMbMB6Qnq1fUKl3/dYbP6T5L9uLixqPD
AuHzzPoURgi4xAfVKedh3WDovbmfzTmxNr49FcQxf9xZ0TV5pJVwtZoqSbfEBbEO3SKf5EO/o9zt
HvrU2IPWkVe2o6ZtLtrWFNvMmjMc+y36zdyI+tNSEiK8osu45ctaTx4DpxLICQtJursEeDaPNJIp
R2BOtWc9ns9X7/hIoJRAktJZ+VHyo44Vfp1h0zL+JUJe48F7hAUR5vNbZb10meeuVuj5/0GAOwDB
4muwNJiZlhq8FEnnuslwZzkhZDuSAtvkQvcWYJxs4nCgIY/wwTRu4HuF2/mpMAIIX8rn8z2031+v
6nmEikG8/GFqKB08BNSBfhFGZCmYwLGXPo2rmwnSIoK8fBJ+3gi6BvS9QA9SAWeuiEg9NKeGWRIe
kAcpszpQTUnZuF0EZLdDexBFkxQZCjU4r/rZ5A+SItR6/zpM3CD1JRhvTmVypzfWyg57XDXsVAEZ
ydmKWqJ6okrajBUtURISnwk2KKMZm76avMnl5Zqg37jEM5BEDHx4qjwHXlhmakjPnHHF3ubXYhup
dQPSsGYi7pSeH9mbK0QcCajoL8isaFv7gIkJyik3oRPq6ayLtX+dH/g6KHVDsQHx4KrHJtv+d0yZ
EbxOKw+JW8XV+B8wNWDZ4qYtv4UBMbiw5wmJg1M07fDne6bi1EXfgxcQvgtb
```

Decryption Key

Submit

Fig4.4: Checking Verification Object


Achieving secure-query results
Achieving secure-query results
Account Storage | DriveHQ
localhost:8084/Achieving_secure_query_results_verification/filedownload.jsp?decrpt_key=g5DBtnQXqfkZ
DATA USER
SEARCH FILES
REQUESTED FILES
LOGOUT
Address
11:34 AM
2/9/2018

command process that allows you to control the computer via commands typed into a text interface. This is what, at one time, scared people away from Linux the most (assuming they had to learn a seemingly archaic command line structure to make Linux work). This is no longer the case. With modern desktop Linux, there is no need to ever touch the command line.   Graphical Server: This is the sub-system that displays the graphics on your monitor. It is commonly referred to as the X server or just �X�. Desktop Environment: This is the piece of the puzzle that the users actually interact with. There are many desktop environments to choose from (Unity, GNOME, Cinnamon, Enlightenment, KDE, XFCE, etc). Each desktop environment includes built-in applications (such as file managers, configuration tools, web browsers, games, etc).   Applications: Desktop environments do not offer the full array of apps. Just like Windows and Mac, Linux offers thousands upon thousands of high-quality software titles that can be easily found and installed. Most modern Linux distributions (more on this in a moment) include App Store-like tools that centralize and simplify application installation. For example: Ubuntu Linux has the Ubuntu Software Center (Figure 1) which allows you to quickly search among the thousands of apps and install them from one centralized location.

Download

Fig4.5: Downloading a File

V. Conclusion

In this paper, we propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can 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. A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

References:

[1] P.Mell and T. Grance, “The nist definition of cloud computing,” http://dx.doi.org/10.602/NIST.SP.800-145.

[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[3] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Springer RLCPS, January 2010.

[4] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposium on Security and Privacy, vol. 8, 2000, pp. 44–55.

[5] E.-J.Goh, “Secure indexes,” IACR ePrint Cryptography Archive, http://eprint.iacr.org/2003/216, Tech. Rep., 2003.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public-key encryption with keyword search,” in EUROCRYPR, 2004, pp. 506–522.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved deinitions and efficient constructions,” in ACM CCS, vol. 19, 2006, pp. 79–88.

[8] M. Bellare, A. Boldyreva, and A. O’Neill, “Deterministic and efficiently searchable encryption,” in Springer CRYPTO, 2007.