Design of Secure and Efficient Product Information Retrieval System Model in Cloud Computing

[1]Mohd Muhibuddin [2] K. Dhanunjayudu
[1]M.Tech Scholar, [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2]Bheema Institute of Technology & Science, Adoni, Kurnool Dist, A.P, India

ABSTRACT

Cloud computing is a promising technique for organizing a vast number of IT resources in a cost-effective and flexible manner. Increasingly many companies are planning to shift their local data management systems to the cloud and uses cloud servers to store and mange product information. A concomitant challenge is determining how to secure the privacy of commercially confidential data while retaining the capacity to search the data. In this paper we propose a privacy-preserving data search scheme for secure and efficient outsourcing and retrieval of product information in cloud computing. We design the proposed scheme and its implementation and analysis results demonstrate the effectiveness of proposed system in terms of security and efficiency in retrieval of product information.

Keywords: cloud server, efficient, cloud computing, product information retrieval, product retrieval feature, secure

I. INTRODUCTION

The ever-increasing number of cyber-transactions has given rise to e-commerce big data. As more data files are kept locally in companies, the strain on local data storage systems grows significantly. Local hardware failures cause significant data destruction or loss, which has a significant impact on the enterprise's day-to-day operations. Fortunately, cloud storage systems arose as a result of such conditions. Cloud computing may collect and arrange a wide range of storage devices using a variety of services such as cluster applications, network technology and distributed file systems[1]. There are already a number of common cloud service products such as Amazon Web Services (AWS), Microsoft Azure (MA), iCloud and App Engine available at home and abroad[2-5]. As huge amounts of data are outsourced to cloud storage servers, traditional plain text-based data search methods are no longer acceptable due to the requirement for data owners to encrypt the aforementioned second and third types of sensitive data. Furthermore, due to network traffic and local storage space limits, users are unable to re-download all of the data to a local disk and later decrypt them for usage. Based on the aforementioned issues [7], privacy-preserving data search algorithms were developed [8-9], with the goal of ensuring that only legitimate users based on identifiers or keywords have access to the data [10-11]. These techniques protect the users' personal information while allowing the server to return to the target ciphertext file based on the query request. As a result, we can ensure the confidentiality and privacy of user data while without adversely affecting query efficiency. We focus on the second and third types of data and design a secure and efficient project data search scheme. The design of encrypted product information outsourcing and retrieval system will be carried out. Further the execution of designed system is performed to illustrate the security and search efficiency of proposed scheme.

The rest of this paper is organized as follows. We first present the proposed retrieval of product information system and algorithm in section 2. Next, the encrypted retrieval of product information scheme is presented in Section 3. Section 4 presents the details of implementation results and discussions. Finally, the conclusion and future work is presented Section 5.

II. PROPOSED RETRIEVAL SYSTEM & ALGORITHM

a) Product Information Retrieval System Model

The design of product information retrieval (outsourcing and searching) system model includes three modules: the data owner, data user and cloud server [12]. The data owner (manager), cloud server and data user's modules are designed using Coding Language: ASP.NET, C#.NET. Figure 1 shows the flow chart for design of every function of modules.

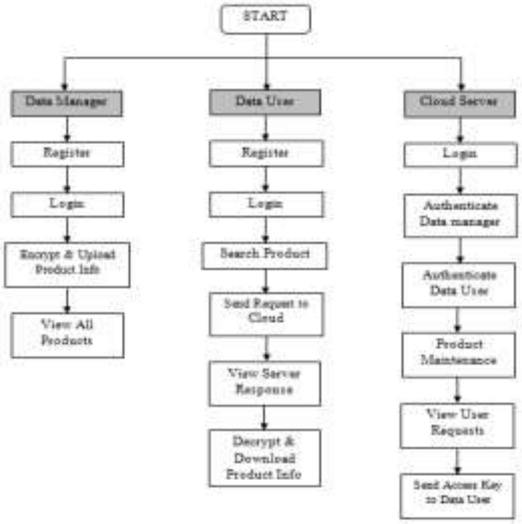


Figure 1: The flow chart for design of proposed system model

Data Manger Module: The function of this module is to manage and collect product information. Also, to improve security it performs encryption of product information file with the use of single secret key before outsourcing the data to the cloud server. Furthermore to improve the search efficiency this module will construct an index structure for the outsourced data. First, an identifying index structure is built using the hash function and a height-balanced binary search tree. The secure kNN algorithm is then used to create a feature vector tree for all of the product's feature vectors.

Data User module: The function of this module is first it creates trapdoor of interest and then it start search for a certain set of products. The trapdoor can be of two types one is the set of hash values and for this type a set encrypted files with the same hash identifiers are returned[13]. Another type of trapdoor is a set of feature vectors and for this the most relevant encrypted files are returned. To obtain the plaintext files the data user has to decrypt the returned files using symmetric secret keys that are provided by the data manager.

Cloud Server Module: This module will be used by data manager to store all data. When data user wants to search some data in the cloud server first a trapdoor has to be generated. This trapdoor must be sent to cloud server. The cloud server will employ a search engine to link data users and encrypted data.

b) Index Structure and Secure kNN Algorithm

Construction of two index structures ID-AVL Tree and Product Retrieval Tree which supports for efficient product retrieval and related search algorithms are proposed to design and implement. A secure kNN algorithm [14] is incorporated in our proposed scheme to provide guaranteed security to outsource data while retaining its search ability.

III. ENCRYPTED PRODUCT INFORMATION RETRIEVAL SCHEME

a) Product Retrieval Tree Construction

To carry out the process of encryption we need to construct product retrieval feature (PRF) tree. This has main parameters: branching factors and threshold and the data owner will preset this parameters. The PRF tree is built incrementally and method of inserting a product vector into the PRF tree is identifying and modifying the appropriate leaf node and then modifying the path from the root node to the leaf node.

b) Retrieval Process of the Interested Products:

In the retrieval process the interested products can be retrieved by data users using identifiers and the identifier is encrypted based on hash function. Then the hash value is sent to cloud server and this value is searched in the ID-AVL tree. If the value is found then the cloud server will send the encrypted product information to data user. Finally the product information is decrypted by user using secret keys and the data retrieval process will be completed. Moreover, the data user interested to search product information using features. First the product feature vector need to be constructed and then a depth first search algorithm for PRF tree and algorithm is to designed

c) Encryption of the Product Retrieval Tree

The two kinds of information are extracted for each product with identifier and product vector and the identifier is encrypted with hash (). The $ID-AVL$ tree construction process is follows. The constructed ID-AVL tree can be easily outsourced to the cloud server because it contains simply a collection of hash values rather than the plaintext identifier. The PRF is constructed on the bases of product vectors and unlike the ID-AVL the PRF tree must be encrypted before being outsourced.

IV. IMPLEMENATAION RESULTS AND DISCUSSIONS

The system modules and algorithms are implemented using tool: MS visual studio 2008 and database: MS SQL SERVER 2005 and results of executions are presented as screenshots.

a) Cloud Server implementation:

The cloud server has been implemented to show the authentication of data manager and data user in cloud. Also it shows the product maintenance in the cloud. The implementation results of these are shown in Figure 2 to Figure 7.

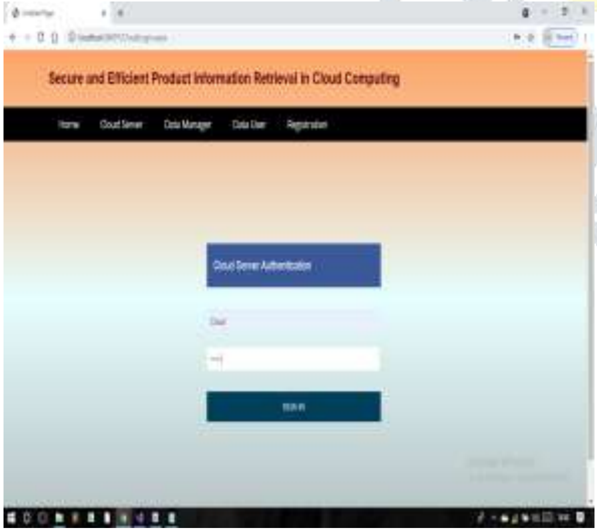

Secure and Efficient Product Information Retrieval in Cloud Computing
Home
Cloud Server
Data Manager
Data User
Registration
Cloud Server Authentication
Cloud
SIGN IN

Figure 2 : Login of cloud server

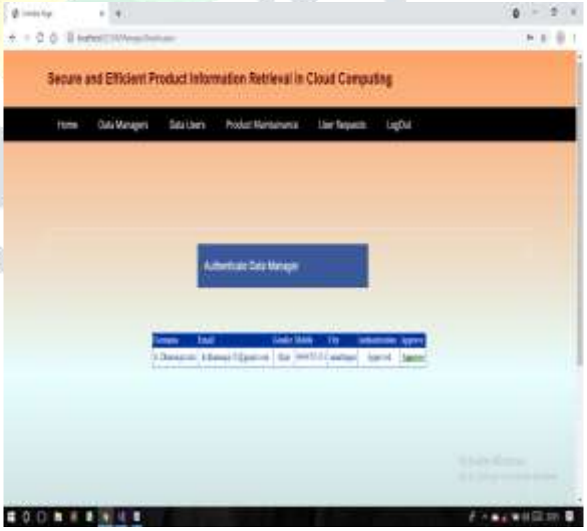
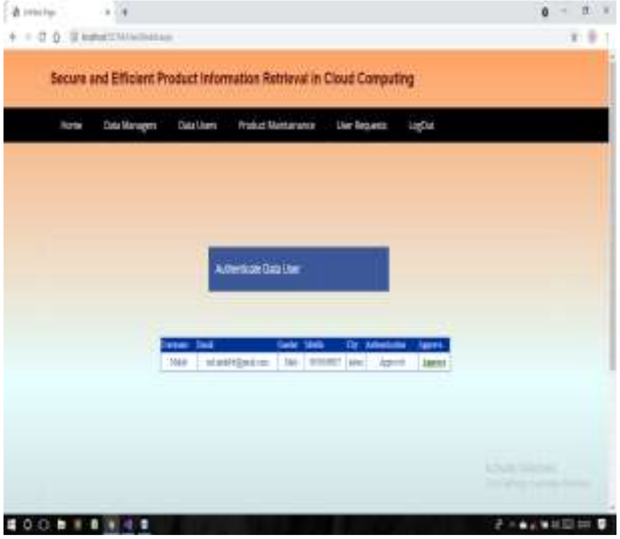

Secure and Efficient Product Information Retrieval in Cloud Computing
Home
Data Managers
Data Users
Product Maintenance
User Requests
LogOut
Authenticate Data Manager
Email

Figure 3 : Authentication of data manager in Cloud

After successfully authenticatiation by cloud server it sends the alert message for data manager Approval



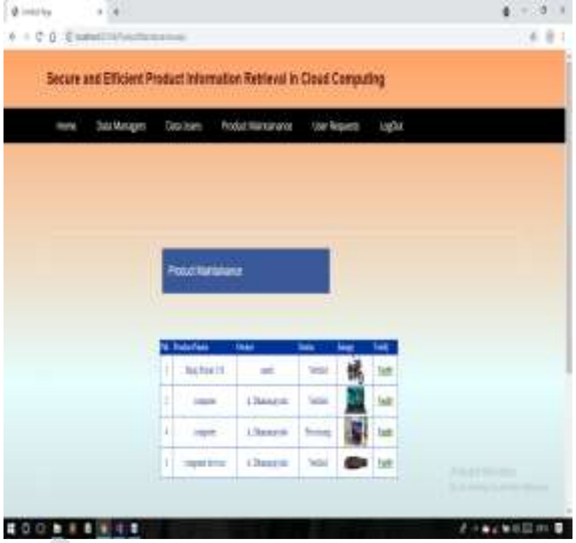
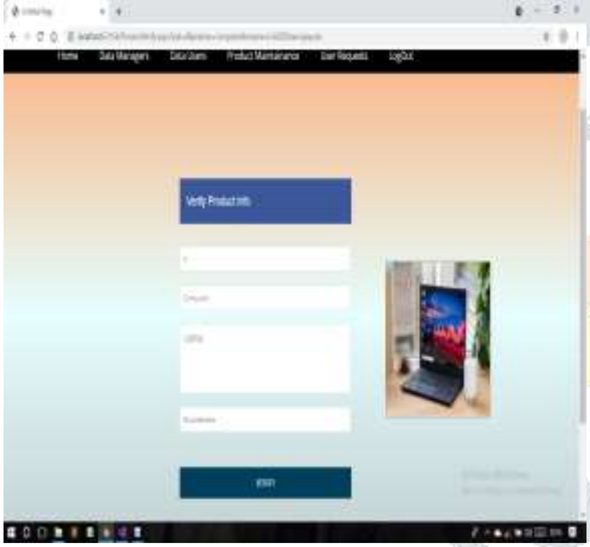


Figure 4: Authentication of data user in Cloud Figure 5: Product mentainence in Cloud

After successfully authenticatiation by cloud server it sends the alert message for data user Approval.



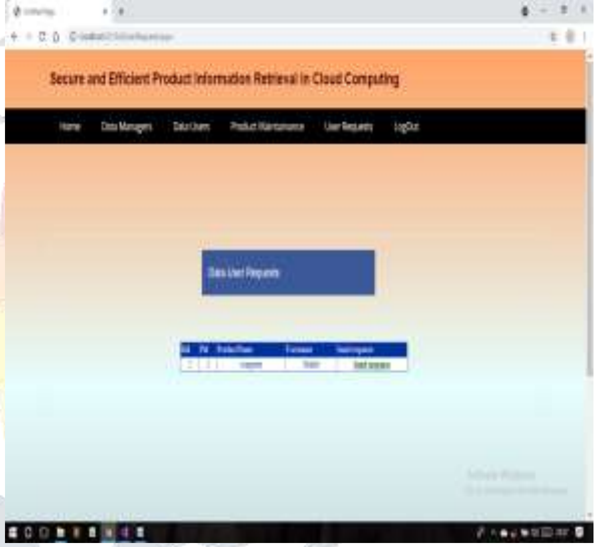
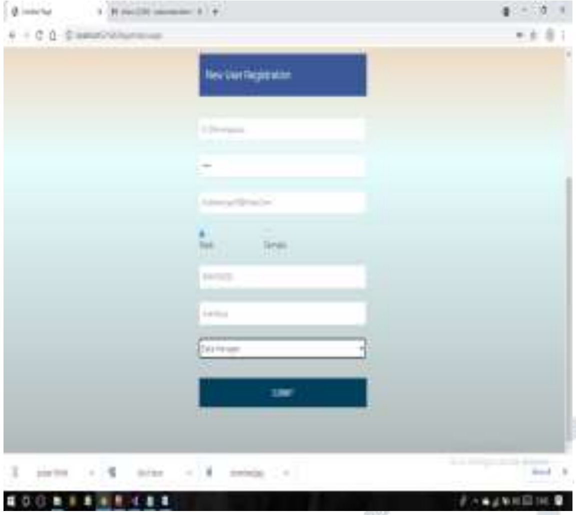


Figure 6: Verifying Product Figure 7: User request for Product in Cloud

The cloud server will do product verification and view the user request and sends access key to data user.

b) Data manager implementation:

The various steps carried out by data manager to upload the product into cloud server are shown in Figure 8 to Figure 11.



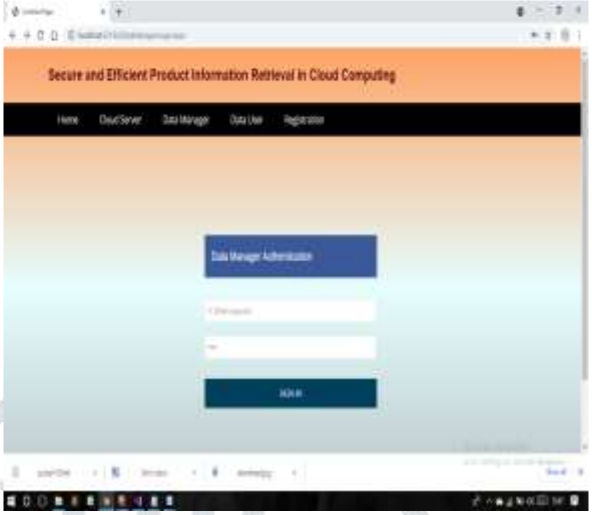
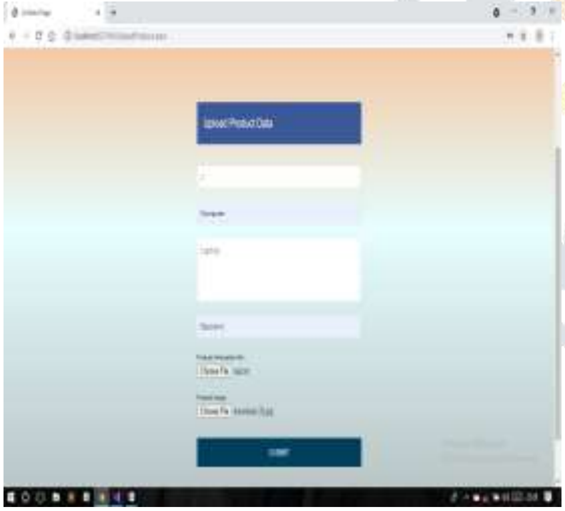

Secure and Efficient Product Information Retrieval in Cloud Computing
Home
Cloud Server
Data Manager
Data User
Registration
Data Manager Authentication
SIGN IN

Figure 8: Data Manager Registration Figure 9: Data Manager Login

First the data manager will do registration as shown in Figure 8 and after successful registration of data manager alert message is sent by cloud about registration success.

Then data user will login to the cloud sever using user name and passed and shown in figure 9.



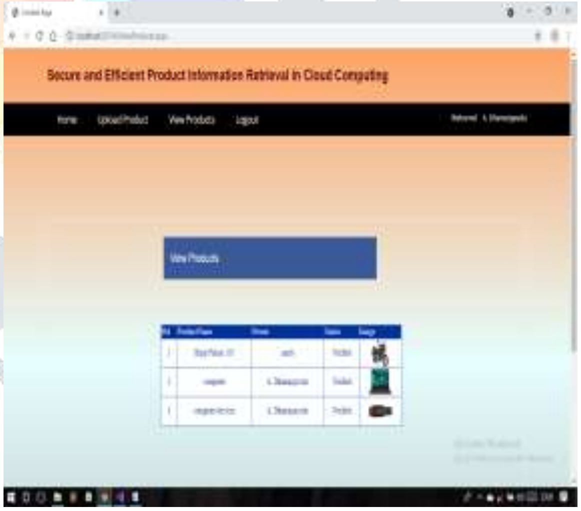

Secure and Efficient Product Information Retrieval in Cloud Computing
Home
Upload Product
View Products
Logout
View Products

Figure 10: Upload Product: Figure 11: View all the Products:

After successful login the data manager will upload product as shown in Figure 10. Finally the data manger will view all the products as shown in Figure 11. An alert message about Product information encrypted and uploaded to cloud is received to data manager.

c) *Data User implementation:*

The various steps carried out by data user are shown form Figure 12 to Figure 17. First step is registration process as shown in Figure 12. Then next step is login process using username and password as shown in Figure 13.

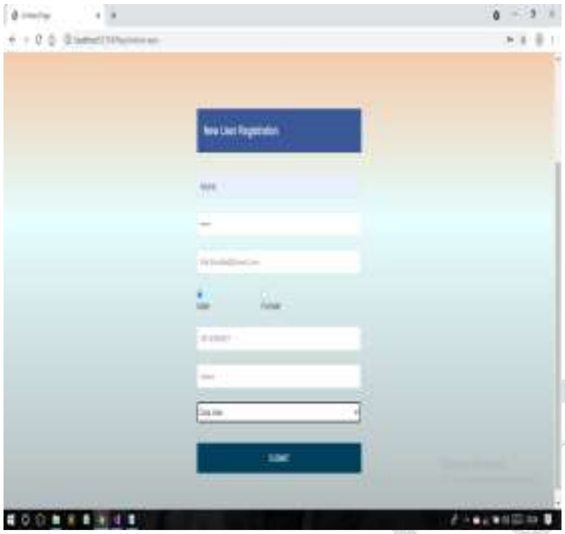


Figure 12: Data User Registration

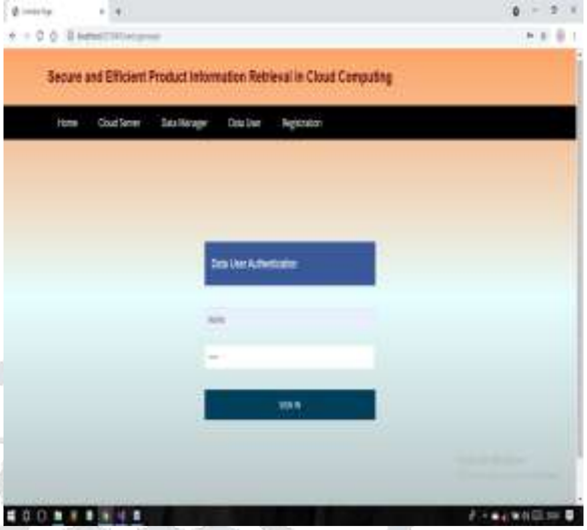


Figure 13: Data user login

Then data user will start searching the product by sending the request to cloud and this is shown in Figure 14. Alert message for sending request to cloud is received to user. After this cloud sends the response and details are shown in Figure 15.

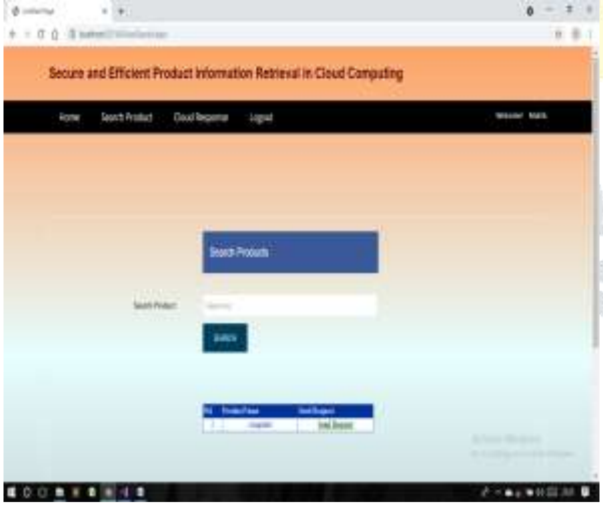


Figure 14: User searching for product

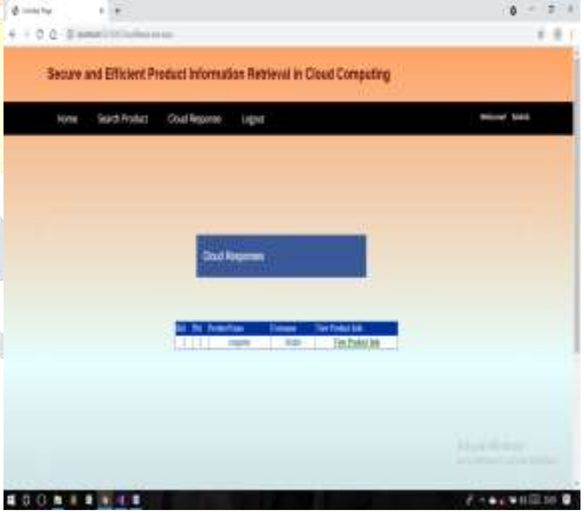


Figure 15: cloud response

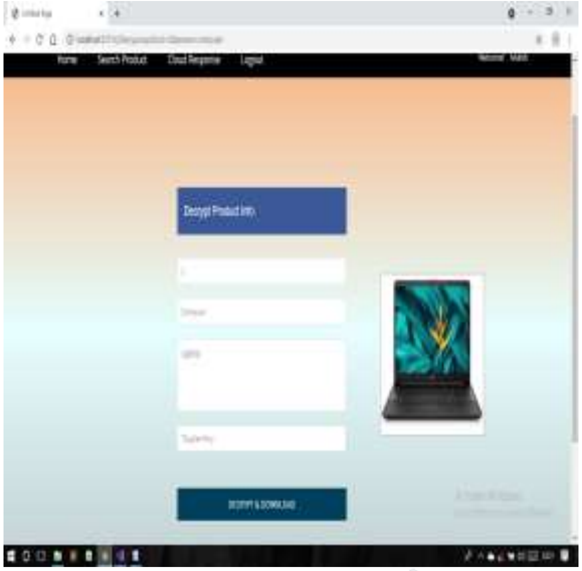
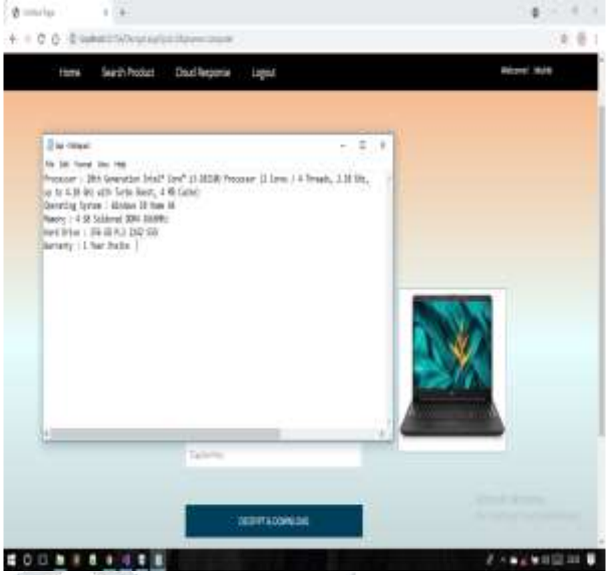


Figure 16: Viewing product information



Processor : 10th Generation Intel® Core™ i3-1005G1 Processor (2 Cores / 4 Threads, 1.20 GHz, up to 3.40 GHz with Turbo Boost, 4 MB Cache)
Operating System : Windows 10 Home 64
Memory : 4 GB Soldered DDR4 2666MHz
Hard Drive : 256 GB M.2 2242 SSD
Warranty : 1 Year Onsite

Figure 17: Downloded decrypted file

Then the user will view the cloud server response and user will decrypt the product and then downloads the file as shown in Figure 16 and Figure 17. All above implementation and analysis results have been demonstrated the effectiveness of proposed system in terms of security and efficiency in retrieval of product information.

V. CONCLUSION AND FUTURE WORK

Conclusion

We have successfully designed and implemented the secure and efficient product information retrieval model and scheme in cloud computing. Also, we have constructed a hash value AVL tree and a product vector retrieval tree and two search algorithms are designed. The product information and vectors are encrypted based on set of independent secret keys and secure kNN algorithm. The execution results and analysis have shown the improved security and efficiency of proposed designed model and scheme.

Future work

In the future, there is scope to suggest standards for overcoming future issues in Cloud security such as physical security, espionage, transparency, data ownership, hypervisor viruses, and malevolent insiders.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication, 800, No.145, pp.7, 2011

[2] Amazon. Amazon S3. Accessed: Sep. 5, 2017, http://aws.amazon.com/s3/

[3] Windows Azure. Accessed: Sep. 5 2017, http://www.microsoft.com/windowsazure/

[4] Apple i Cloud. Accessed: Sep. 5, 2017, Available: http://www.icloud.com/

[5] Google App Engine. Accessed: Sep. 5, 2017, Available: http://appengine.google.com/

[6] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, no. 3 pp. 583- 592, 2012.

[7] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, Vol. 34, no. 1, pp. 1-11, 2011.

[8] Y. Li, Y. Yu, B. Yang, G. Min and H. Wu, "Privacy preserving cloud data auditing with efficient key update," Future Gen. Computer Systems, Elsevier, Vol. 78, pp.789-798, 2018.

[9] D. X. Song and D. A. Wanger Perrig, ``Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, pp: 44-55, 2000.

[10] C. Chen et al., ``An efficient privacy-preserving ranked keyword search method," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 4, pp. 951_963, Apr. 2016.

[11] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ``Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546_2559, Sep. 2016.

[12] Y. Zhao and Q. Zeng, "Secure and Efficient Product Information Retrieval in Cloud Computing," in IEEE Access, vol. 6, pp. 14747-14754, 2018,

[13] H. S. Rhee, J. H. Park, W. Susilo, & D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," J. Syst. Softw., vol. 83, no.5, pp.763-771, 2010.

[14] W. K. Wong, D. W. L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2009, pp. 139-152.