IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SECURE CLOUD -STORAGE WITH FILE ACCESS AND FILE SHARING CONTROL

[1] E.Chitti Babu, [2] S.Vamsi Krishna Yadav

[1]Faculty, [2]Student

Computer Science Department,

Geethanjali Institute of Science and Technology,Nellore

***Abstract*—** Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low-cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.

***Index Terms*—**Cloud storage, Secure storage, dual access control.

## I. INTRODUCTION

In the recent decades, cloud-based storage service has attracted considerable attention from both academia and industries. It may be widely used in many Internet-based commercial applications (e.g., Apple iCould) due to its long-list benefits including access flexibility and free of local data management. Increasing number of individuals and companies nowadays prefer to outsource their data to remote cloud in such a way that they may reduce the cost of upgrading their local data management facilities/devices. However, the worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service. In many practical applications, outsourced data may need to be further shared with others. For example, a Dropbox user Alice may share photos with her friends. Without using data encryption, prior to sharing the photos, Alice needs to generate a sharing link and further share the link with friends. Although guaranteeing some level of access control over unauthorized users (e.g., those are not Alice's friends), the sharing link may be visible within the Dropbox administration level (e.g., administrator could reach the link).Since the cloud (which is deployed in an open network) is not be fully trusted, it is generally recommended to encrypt the data prior to being uploaded to the cloud to ensure data security and privacy. One of the corresponding solutions is to directly employ an encryption technique (e.g., AES) on the outsourced data before uploading to cloud, so that only specified cloud user (with valid decryption key) can gain access to the data via valid decryption.To prevent shared photos being accessed by the "insiders" of the system, a straightforward way is to designate the group of authorized data users prior to encrypting the data. In some cases, nonetheless, Alice may have no idea about who the photo receivers/users are going to be. It is possible that Alice only has knowledge of attributes w.r.t. photo receivers. In this case, traditional public key encryption (e.g., Paillier Encryption), which requires the encryptor to know who the data receiver is in

advance, cannot be leveraged. Providing policy-based encryption mechanism over the outsourced photos is therefore desirable, so that Alice makes use of the mechanism to define access policy over the encrypted photos to guarantee only a group of authorized users is able to access the photos.In a cloud-based storage service, there exists a common attack that is well-known as resource-exhaustion attack. Since a (public) cloud may not have any control over download request (namely, a service user may send unlimited numbers of download request to cloud server), a malicious service user may launch the denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks to consume the resource of cloud storage service server so that the cloud service could not be able to respond honest users' service requests. As a result, in the "pay-as-you-go" model, economic aspects could be disrupted due to higher resource usage. The costs of cloud service users will rise dramatically as the attacks scale up. This has been known as Economic Denial of Sustainability (EDoS) attack which targets to the cloud adopter's economic resources. Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g., file size). Therefore, an effective control over download request for outsourced (encrypted) data is also needed.In this paper, we propose a new mechanism, dubbed dual access control, to tackle the above aforementioned two problems. To secure data in cloud-based storage service, attribute-based encryption (ABE) [9] is one of the promising candidates that enables the confidentiality of outsourced data as well as fine-grained control over the outsourced data.

In particular, Ciphertext-Policy ABE (CP-ABE) [5] provides an effective way of data encryption such that access policies, defining the access privilege of potential data receivers, can be specified over encrypted data. Note that we consider the use of CP- ABE in our mechanism in this paper. Nevertheless, simply employing CP-ABE technique is not sufficient to design an elegant mechanism guaranteeing the control of both data access and download request.

A strawman solution to the control of download request is to leverage dummy ciphertexts to verify data receiver's decryption rights. It, concretely, requires data owner, say Alice, to upload multiple "testing" ciphertexts along with the "real" encryption of data to cloud, where the "testing" ciphertexts are the encryptions of dummy messages under the same access policy as that of the "real" data. After receiving a download request from a user, say Bob, cloud asks Bob to randomly decrypt one of the "testing" ciphertexts. If a correct result/decryption is returned (i.e.indicating Bob is with valid decryption rights), Bob is authorized by Alice to access the "real" data, so that the cloud allows Bob to download the corresponding ciphertext. Nevertheless, several disadvantages of the above approach may be identified as follows. First of all, the data owner, Alice, is required to encrypt a number of dummy ciphertexts under the same policy as the "real" ciphertext. This may yield a considerable computational overhead for Alice, which may bring inconvenience in practice, for example, Alice just wants to upload one photo to iCloud from her cellphone, but needs to prepare more than one ciphertexts. Second, all ciphertexts, including dummy ones, are uploaded to cloud at the same time. This inevitably imposes extra cost on network bandwidth (as well as prolonging data uploading time), which may not be applicable to some service users whose cellular network is under pay-as-you-go plan or equipped with old generation of broadband cellular network technology (e.g., 3G). Third, a data receiver/user, Bob, has to additionally decrypt a random-chosen "testing" ciphertext from cloud, as a test of his valid download request. As a result, Bob has to "pay" double (decryption price) for accessing to the "real" data, which again may not be scalable in resource constrained setting.

## II. LITERATURE REVIEW

1. Cloud Computing Security : From DDoS to EDoS

Economic denial of sustainability (EDoS) appeared to be a new menace of cloud computing. This pristine attack is a breed of DoS or DDoS attack that targets the vulnerabilities of cloud consumers utility pricing model. EDoS attackers steadily send illegitimate traffic to gradually consume cloud resources such as virtual machines

2. Outsourced attribute based encryption with keyword search function for cloud storage

Cloud computing becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing intended data users to retrieve these data stored in cloud. This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and ciphertext size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-

grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP)

3. Full verifiability for outsourced decryption in attribute based encryption.Yichen Zhang, and Jinguang Han.

Attribute based encryption (ABE) is a popular cryptographic technology to protect the security of users' data. However, the decryption cost and ciphertext size restrict the application of ABE in practice. For most existing ABE schemes, the decryption cost and ciphertext size grow linearly with the complexity of access structure. This is undesirable to the devices with limited computing capability and storage space. Outsourced decryption is considered as a feasible method to reduce the user's decryption overhead, which enables a user to outsource a large number of decryption operations to the cloud service provider (CSP). However, outsourced decryption cannot guarantee the correctness of transformation done by the cloud, so it is necessary to check the correctness of outsourced decryption to ensure security for users' data.

4. A proposal for an iso standard for public key encryption.Victor Shoup

We proposed a privacy-aware multi-context RFID infrastructure that employs puic key cryptography (PKC). In this infrastructure, different readers can interrogate RFID tags for different purposes. It is not possible for the readers to track RFID tags, therefore their privacy is preserved. During interrogation, tags encrypt their IDs with the public key of the backend server, which performs only one decryption to access the ID of the interrogated tag. In symmetric cipher-based schemes.

## III. METHODOLOGY

The proposed system for detecting brain tumors would use computer programs to look at medical images of the brain(MRI) and determine if there are any tumors present. The system would first clean up the images to make them clearer, then separate the brain from the rest of the image. It would then use a special type of computer program to find patterns in the image that could indicate the presence of a tumor. Once the computer program is trained to recognize the different types of tumors, it would be able to automatically detect and identify glioma, meningioma, and pituitary tumors in new images.

Advantages of proposed system:

The proposed system for detecting three types of brain tumors (glioma, meningioma, and pituitary tumors) has several advantages over traditional diagnostic methods:

Accurate Diagnosis: The proposed system uses CNN to accurately detect and classify brain tumors. This can help doctors make more accurate diagnoses and plan more effective treatment strategies.

Efficiency: The proposed system can quickly and efficiently process medical images, reducing the time it takes to diagnose and treat brain tumors. This can lead to faster treatment and better patient outcomes.

Cost-effective: The proposed system can potentially reduce healthcare costs associated with the diagnosis and treatment of brain tumors. By accurately detecting brain tumors early on, the system can help avoid costly treatments and procedures later on.

A system for brain tumor detection typically involves the use of medical imaging technologies such as magnetic resonance imaging (MRI). This imaging technique generate high-quality images of the brain, which can be analyzed using advanced algorithms and machine learning models to detect the presence of tumors.

Segmenting tumors from MRI brain images is a challenging task that requires accurately identifying the region of interest within an object. It is considered ambitious due to the complex nature of brain tumors and the large amount of data involved. Brain tumor segmentation is a critical step in medical image processing as tumors can have soft tissue boundaries and may not be well-defined. Image processing techniques are used to enhance the quality of MRI images and extract features for classification. The image processing steps for brain tumor segmentation include skull stripping, pre-processing, and tumor contouring, among others.

The implementation process includes the uploading the image which is the random image to test the type of tumor.At first the model should be trained to detect the tumor. It will be trained by using a dataset from Kaggle that contains MRI images of brain with four categories (Glioma, Meningioma, Pituitary and No Tumor) of separation in it. The model is trained by taking each image through the CNN layer. After training the model with all the images in the dataset, it will be saved in a preferred location.Secondly, the image need to be provided to test, an interface will be available to take the input from the user which is the MRI image of brain. This interface was designed using TKinter. The saved model will predict the presence of tumor and classify the type of tumor. Then this result will be displayed to the user. If there is an image that is not belonging to four classes then the matrix values closer to the values of particular class will be displayed.

## IV. CONCLUSION

In this project, we used Convolutional Neural Networks(CNN) to train the brain tumor classifying model by giving it the required dataset and after training we can use this model to predict the type of brain tumor from new brain MRI(magnetic resonance imaging) images. It is able to detect three types of tumors which are Glioma, Meningioma and Pituitary respectively. If there is no presence of tumor in it, it gives no tumor as output. So it contains four classes. Our training accuracy was 86% and our prediction accuracy is nearly 98%.If there is presence of other type of tumor this model gives the nearest tumor class as output, with the right quality images our model can detect Glioma, Meningioma and Pituitary tumors accurately.

## REFERENCES


1) Deepak, S., and P. M. Ameer. "Brain tumour classification using deep CNN features via transfer learning." Computers in biology and medicine 111 (2019): 103345.
2) L. Zhou, Z. Zhang, Y.C. Chen, Z.Y. Zhao, X.D. Yin, H.B. Jiang, A deep learning-based radionics model for differentiating benign and malignant renal tumours, Transl, Oncol. 12 (2) (2019) 292–300.
3) Hemanth, G., M. Janardhan, and L. Sujihelen. "Design and Implementing Brain Tumour Detection Using Machine Learning Approach." In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1289-1294. IEEE, 2019.
4) Smirnov, Evgeny A., Denis M. Timoshenko, and Serge N. Andrianov. "Comparison of regularization methods for imagenet classification with deep convolutional neural networks." Aasri Procedia 6 (2014): 89-94.
5) Wu, Songtao, Shenghua Zhong, and Yan Liu. "Deep residual learning for image steganalysis." Multimedia tools and applications 77, no. 9 (2018): 10437 10453.
6) Szegedy, C., S. Ioffe, V. Vanhoucke, and A. Alemi. "Inception-ResNet and the Impact of Residual Connections on Learning." arXiv preprint arXiv:1602.07261.
7) Noh, Hyeonwoo, Seunghoon Hong, and Bohyung Han. "Learning deconvolution network for semantic segmentation." In Proceedings of the IEEE international conference on computer vision, pp. 1520-1528. 2015.
8) Chen, Liang-Chieh, George Papandreou, Iasonas Kokkinos, Kevin Murphy, and Alan L. Yuille. "Semantic image segmentation with deep convolutional nets and fully connected crfs." arXiv preprint arXiv:1412.7062 (2014).
9) Swati, Zar Nawab Khan, Qinghua Zhao, Muhammad Kabir, Farman Ali, Zakir Ali, Saeed Ahmed, and Jianfeng Lu. "Brain tumour classification for MR images using transfer learning and fine-tuning." Computerized Medical Imaging and Graphics 75 (2019): 34-46.
10) Bernal, Jose, Kaisar Kushibar, Daniel S. Asfaw, Sergi Valverde, Arnau Oliver, Robert Martí, and Xavier Lladó. "Deep convolutional neural networks for brain image analysis on magnetic resonance imaging: a review." Artificial intelligence in medicine 95 (2019): 64-81.
11) Sobhaninia, Zahra, Safiyeh Rezaei, Alireza Noroozi, Mehdi Ahmadi, Hamidreza Zarrabi, Nader Karimi, Ali Emami, and Shadrokh Samavi. "Brain tumour segmentation using deep learning by type specific sorting of images." arXiv preprint arXiv: 1809.07786 (2018).
12) Cui, Shaoguo, Lei Mao, Jingfeng Jiang, Chang Liu, and Shuyu Xiong. "Automatic semantic segmentation of brain gliomas from MRI images using a deep cascaded neural network." Journal of healthcare engineering 2018 (2018).
13) Özyurt, Fatih, Eser Sert, and Derya Avcı. "An expert system for brain tumour detection: Fuzzy C-means with super resolution and convolutional neural network with extreme learning machine." Medical hypotheses 134 (2020): 109433.
14) Ostrom, Quinn T., Gino Cioffi, Haley Gittleman, Nirav Patil, Kristin Waite, Carol Kruchko, and Jill S. Barnholtz-Sloan. "CBTRUS statistical report:primary brain and other central nervous system tumours diagnosed in the United States in 2012–2016." Neuro-oncology 21, no. Supplement_5 (2019): v1-v100.