Secure Data Access using Hierarchical Key Assignment Schema in Cloud Computing

Vaibhav S. Patil,
Dept. of CSE, KLS's Gogte Institute of Technology, Belagavi, India
Visvesvaraya Technological University, Belagavi

Umesh M. Kulkarni,
Dept. of CSE, KLS's Gogte Institute of Technology, Belagavi, India
Visvesvaraya Technological University, Belagavi

Harish H. Kenchannavar,
Dept. of ISE, KLS's Gogte Institute of Technology, Belagavi, India
Visvesvaraya Technological University, Belagavi

Abstract

The field of cloud computing is gaining more and more importance in IT world. There are numerous distributed systems in a cloud environment interconnected to deliver cloud resources over the internet. There are gradually more security and privacy concerns with outsourced data in the cloud as a result of this new paradigm requires that ensure the protection of user's data on cloud. The data on a cloud server should be encrypted to maintain its confidentiality. Building scalable access control for data storage and removing access rights from unauthorized users. This work presents a hierarchical key assignment schema used to provide security to user's data and its process. In this, there is user authentication providing a private key to that user after registration and a secret key for every process with cloud service provider authentication. In real-time 128-bit AES algorithm is used to store and retrieve the data from the cloud, however it is publicly available hence chances of data decryption from a third party are more, to overcome this a 10-bit alpha-numeric string is encrypted and sent along with the user's encrypted file to the cloud. This provides zero-knowledge encryption to that user's data.

Keywords:Hierarchical key assignment, Advanced Encryption Standard (AES), zero-knowledge encryption.

I.INTRODUCTION

The on-demand availability of computer system resources, in particular data storage and processing power, without direct active supervision by the user is known as cloud computing. Functions in large clouds are frequently dispersed over several sites, each of which is a data centre.

Both the academic community and the information technology sector are paying close attention to cloud computing. This new computing paradigm, which is based on parallel and distributed computing architecture, has many benefits, including cheap cost, high efficiency, flexibility, and scalability. Three delivery types for cloud computing infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) can be separated from the base layer to the top layer. Today, a variety of cloud service platforms, like Amazon's EC2, Google App Engine, Microsoft's Azure, IBM's Blue Cloud, etc., offer services through the Internet. Enterprise customers will be able to access cloud resources anytime, anyplace, and without having to handle the underlying hardware/software systems thanks to the anticipated advancements of cloud service systems.

Data is without a doubt a vital resource for all organisations, particularly for enterprise users. But in the age of cloud computing, this merits further attention. In contrast to traditional local storage methods, cloud computing uses the Internet to access servers that are located elsewhere to store data. Data must be uploaded by the data owner onto the cloud server before it can be retrieved by authorised users. Data confidentiality is the main worry with regard to cloud computing because the semi-trusted Cloud Service Provider (CSP) is in charge of managing the cloud and all of the data on it. While encryption can ensure data secrecy, traditional encryption techniques by themselves cannot satisfy a requirement in many cloud storage applications, namely flexible and granular data access control.

With the use of cloud computing, clients from all over the world can access services, computational power, and data storage facilities. There are four different kinds of clouds: private, public, community, and hybrid. Numerous features of cloud computing include scalability, pay-per-use, resilience, and agility. Scalability, lower IT costs, flexibility, business continuity, practically infinite storage, and other benefits are all associated with cloud computing. There are a lot of issues with the growth of cloud computing. Due to its reliance on internet-based services, cloud computing has two major problems: data security and access control. The process through which a user can access data from cloud servers is known as an access control. Using an effective and secure access control paradigm, the system, the CSP, or the data owner can limit illegal data access and ensure data confidentiality for user's sensitive data. Traditional access control models in cloud computing typically presuppose that the data owner and the CSP are in the same trusted domain. The data owner and the CSP are often in two different domains in cloud computing, so this assumption is incorrect nowadays. Since the data owner and the CSP are not in the same domain, the data owners keep their data or files on other domains in encrypted form so that they can be safely shared with CSPs of various domains.

II. RELATED WORK

In [1] an approach to flexible and fine-grained hierarchical access control in cloud computing is presented using a hierarchical key assignment mechanism based on linear geometry. The suggested technique is a direct access scheme for hierarchical access control, meaning that

without the requirement for repetitive computation, any class at a higher level in the hierarchy can immediately determine the encryption key of its descendant class.

In [2] ensure data privacy and usability in cloud computing, secure search over encrypted remote data is essential. In a multi-user system, fine-grained access control is required to prevent unauthorised data consumption. However, a trusted user could purposefully reveal the secret key to gain financial advantage. Therefore, it is urgent to find and ban the malicious user who misuses the secret key.

[3] In cloud computing, an effective file hierarchy attribute-based encryption approach is suggested. The layered access structures are combined into a single access structure, and the combined access structure is then used to encrypt the hierarchical files. The files might share the attributes-related ciphertext components. As a result, both ciphertext storage and encryption time are reduced.

In [4] a cloud computing environment, this paper discusses several data security and privacy protection concerns and suggests a technique for delivering security services including authentication, authorisation, and confidentiality as well as monitoring in real time. Using the 128 bit Advanced Encryption Standard (AES), data security and confidentiality are improved. In the suggested method, data is encrypted with AES before being uploaded to the cloud. The suggested methodology prevents unwanted access to user data by using a Short Message Service (SMS) alarm system.

Overview of the survey

The literature review articles were studied for this paper and it was discovered that two-factor authentication is basically used. Hierarchical access control is an ongoing process. Most of the cloud service providers use 128-bit AES encryption because of time efficiency. Data encryption using the AES algorithm is publicly available. Many CSPs do not provide zero-knowledge encryption to the data owners.

In this project, we have done everything to overcome the limitation from the other paper which is the hierarchical key assignment schema is used which is user authentication, for every user login a unique secret key is assigned to that user with owner authentication. When the user finally wants to upload the file, the file will be encrypted with 128-AES encryption and sent along with the encrypted secret key. This results in only the authentic user only access this file and using the secret key they can decrypt the file. This avoids the interruption of third party into user's data and eventually provide zero-knowledge encryption.

2.1 Problem Identification

Referring above papers we found that most of the cloud service providers are using a 128-bit AES algorithm which is publicly available, so anyone can easily decrypt the 128-bit AES encrypted file. Providing security for the data which is stored on cloud is an ongoing process.

2.2 Problem Definition

Designing secured access to cloud services using Hierarchical Key Assignment Schema with the help of two-factor authentication and storing/retrieving the data using 128-bit AES encryption/decryption method to provide zero-knowledge encryption.

2.3 Objectives

1. Providing secured access control with the help of Hierarchical Key Assignment Schema.
2. File upload with 128-bit AES encryption along with encrypted user's private key.
3. Providing zero-knowledge encryption for the stored data on cloud.

2.4 Technology Used

- Java (Java Swing)
- NetBeans
- XAMPP Server
- MySQL
- CloudSim

III.METHODOLOGY AND IMPLEMENTATION

This chapter briefs about the methodology employed in the implementation of secure data access in cloud computing. After referring to the research paper's, we found that most of the cloud service providers are using a 128-bit AES algorithm which is publicly available if any hacker hacks and gets access to stored cloud data he can easily decrypt the files.

To overcome this problem first we grant permission to the authorized user's only and for every user login a 10-bit secret key will be assigned which regenerates every single time. Providing security to the stored data is done by encrypting user's data with 128-bit AES algorithm and sent along with the 10-bit encrypted private key so that only a particular user can decrypt that file. This method provides zero-knowledge encryption to the user's data.The 128-bit AES algorithm is already in use because of this time efficiency. Along with 128-bit AES encryption, we added user's private key encryption for better security for stored data.

We particularly used a hierarchical key assignment schema that provides security keys for user, cloud service providers and users processes. There are mainly three times where the private and security keys are generated. When the user register himself at the beginning of the process first private key will be generated and that key is fixed for that user. At the time of every login one secret key will be generated and which is used only once. This secret key provides secure operations so that any unauthorized entity cannot interfere user's processes. The last key is generated for the cloud service provider so that using this key we are allowed to store the data in cloud storage. The users are identified by CSP only but they are unknown to the cloud server, this key will ensure that we are an authentic user from a particular cloud service provider. The main obstacle we faced is that this all process will happen at the backend while storing any data on the cloud server, to display every step we require many templates. The cloud simulator also provides a limited number of changes otherwise default cloudsim will perform all these tasks at the backend only.

Consider figure 1 when the user wants to access the cloud server, he has to register himself and then he can login to the system. The user will be provided with a private 10-bit pseudo-random key at the time of registration. When the user login with an e-mail id and password if

it is an authentic user then only he is allowed otherwise his request will be cancelled.The central authority will give the temporary secret key for that instance so that the user performs his operation securely.When the upload/download request is sent to the cloud service provider, the CSP will authenticate this process and valid users are only allowed to do further tasks like file upload to the cloud server or download files from the cloud server.

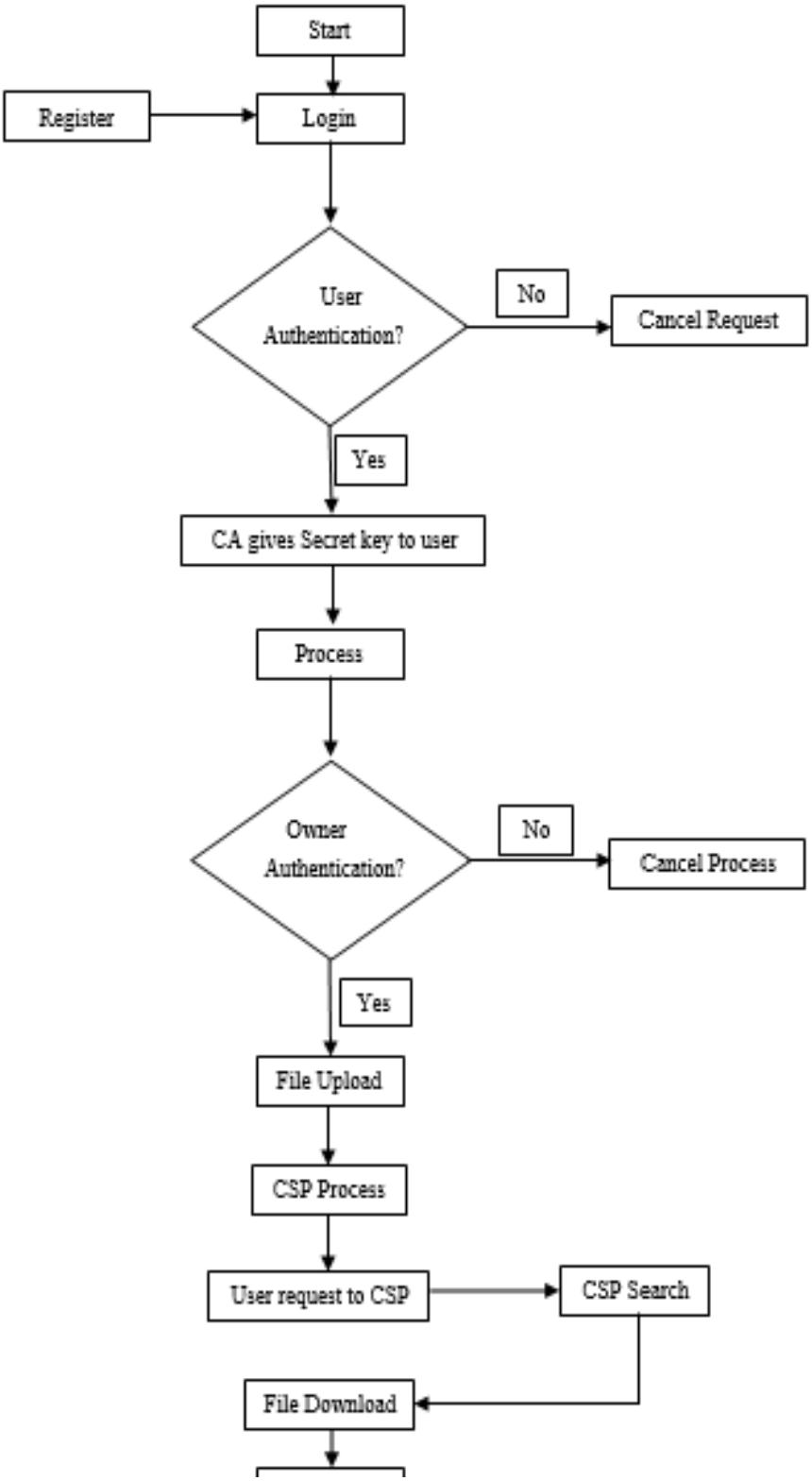

Figure 1: Flow chart of secure data access

As shown in Figure 2 a hierarchical access control system in cloud computing consists of two kinds of entities data owner and CSP. Cloud service acts as an intermediate between the data owner and the cloud storage. CSP will take a huge amount of storage area in the cloud and according to user requests it allows them to use it. CSP will take charges for its service to user. Pay per use is the method by which both the user and CSP benefited.

Consider a scenario where a data owner wants to upload its file to the cloud. He will register himself on a cloud service provider for cloud services. For every user a private key is assigned and for every operation a secret key is assigned so that only an authentic user can access the services. The user will send his file to the cloud but at the backend, the file will be encrypted by a 128-bit AES algorithm and one 10-bit encrypted secret key is added along with it for better security. The cloud service provider is having its own secret key acting as an authentic connection between user and cloud storage. After successful completion of these steps, the file is stored on the cloud and thus provides zero-knowledge encryption.

The same steps are followed in reverse order to download the file from the cloud storage.

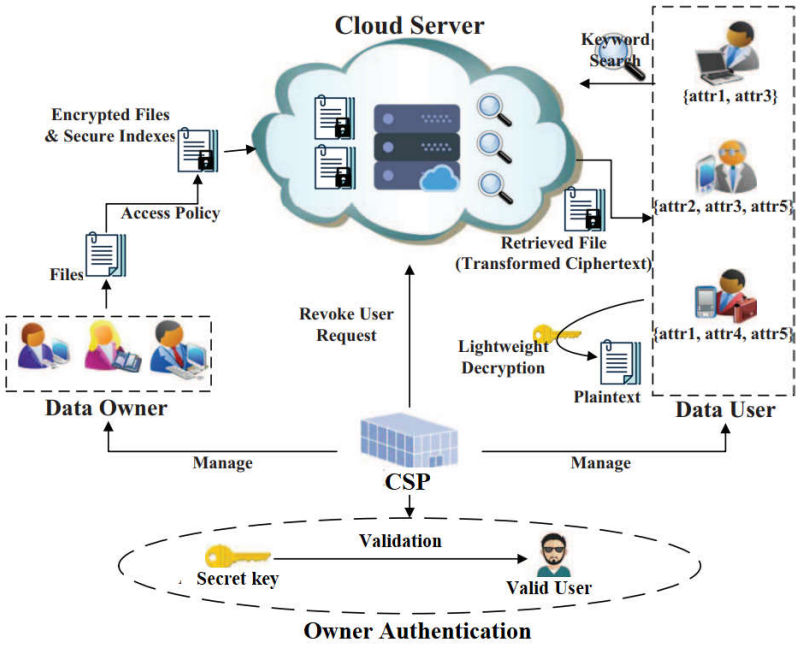

Figure 2: System Architecture

3.1 Modules:

- User Login.
- Get Secret Key.
- Process.
- File Upload.
- CSP Process.
- File Download.

3.2 Modules Description:

User Login

Users can login with their email id. First, the user has to register with their email id and password and after successful registration user can login to perform required operations. The user has to set a strong password including small and capital alphabet, numbers, special characters and total password length should be equal to or greater than eight characters. This provides the first step in the key hierarchy by avoiding weak passwords.

Get Secret Key

Get Secret Key Process is one of the use authentications. Central Authority (CA) verifies the user details and gives the secret key for that user. It is very important to access the controls of the data owner. The user gives that secret key to the data owner then the data owner gives the access controls to the user. The secret key is an alphanumeric key of length 10. Which is automatically generated when the user register. This secret key is given at once when the user register and a secret key is generated for every single login of the user.

Process

Users can choose between a file download and an upload process. This dynamic key management system is specialized. In contrast to traditional local storage, cloud computing uses the Internet to store data on servers that are located elsewhere. Access control is forced to deal with the need for various and flexible access privileges as group-oriented applications evolve.

File Upload

The user must upload their own data to the cloud server, and only authorised users are able to access the data once it has been stored there. While encryption can ensure data secrecy, traditional encryption techniques by themselves cannot satisfy a requirement in many cloud storage applications, namely flexible and granular data access control. To ensure that only the user can decrypt the uploaded file, it is encrypted using the 128-bit AES technique and transmitted with an encrypted secret key. This forbids unauthorised access to user data.

CSP Process

Data confidentiality is the top problem in cloud computing because a cloud service provider (CSP) is responsible for managing the cloud and all of the data on it. It responds to each class's access requests and keeps both encrypted data and publicly available information. Additionally, CSP has a secret key that only it may use to access the cloud storage.

File Download

Data must be downloaded by the user into the cloud server before it can be accessed by authorised users. A reverse 128-bit AES algorithm and a user secret key are used to decrypt the file.

IV. RESULT AND ANALYSIS

The main objective of my project was the use of a hierarchical key assignment schema for user authentication and encrypting the user data with the help of 128-bit AES encryption along with a 10-bit encrypted users security key.

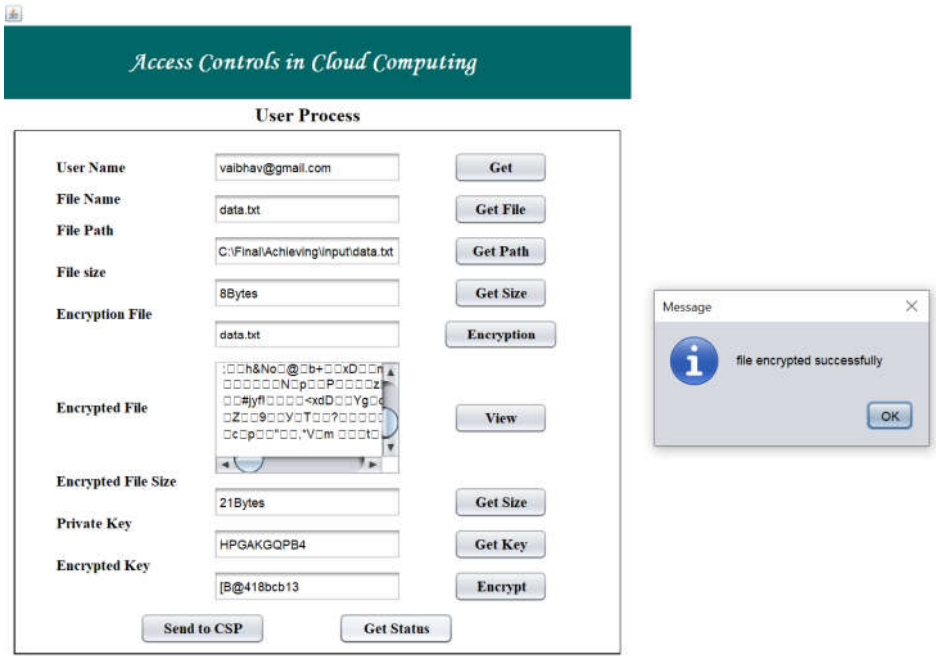

Figure 3: User Process Page.

The figure 3 shows file name data.txt and the private key is encrypted prior to upload on cloud storage.

The file is first selected by users then the file path and its size are calculated. Then the file is encrypted with 128-bit AES encryption. The encrypted file is sent along with a 10-bit pseudo-random number which is also encrypted and sent along with the encrypted file. The main aim is to provide security to the stored file and only an authentic user can decrypt this file using his private key. No one other than the valid user cannot decrypt the file hence providing zero-knowledge encryption.

In this work when the user wants to perform a file upload or download operation, he has to register himself and login into the system. Users can login with their email id. First, the user has to register with their email id and password and after successful registration user can login to perform required operations. The user has to set a strong password including small and capital alphabet, numbers, special characters and the total password length should be equal to or greater than eight characters. This provides the first step in the key hierarchy by avoiding weak passwords. At the time of registration, the user is assigned a permanent private key and asked to set a strong password. When the user login he will be assigned a temporary secret key for that particular instance. When the user enters all the required credentials for login, all the entered information is crosschecked for authentication and only authentic users are allowed to do the further process. The unauthentic user requests are cancelled.

All the private and secret key generation is done by the central authority. When the user login Central Authority (CA) verifies the user details and gives the secret key for that user. The secret key is an alphanumeric key of length 10. Which is automatically generated when the user register. This secret key is given at once when the user register and a secret key is generated for every single login of the user. Whereas central authority will generate a total of 3 keys particularly, a private key for each user which is a permanent, secret key for each login of the user and one owner private key for each user so that cloud storage can identify from which cloud service provider the user belongs.

Owner authentication is done by the owner's private key which acts as a connecting link between the user and cloud storage. If the user fails to satisfy this condition, then the process will be cancelled. The owner's private key is matched with the stored owner key on the cloud and only genuine user will be allowed to access the cloud storage.

The process is where the user has to decide whether he has to upload or download a file. For the first time the user selects file upload. The selected file will be encrypted by 128-bit AES encryption and sent along with the encrypted user's private key. The main purpose of the addition of encrypted user's private key is to provide greater security in terms of zero-knowledge encryption. By any chance if anyone other than the genuine user gets this encrypted file, he cannot decrypt it in spite of knowing that it is encrypted by the AES algorithm because of this encrypted user's private key. The cloud service provider also cannot view the file because of this kind of encryption.

Cloud Service Provider (CSP) manages the cloud and all data on the cloud and as a result, data confidentiality is at the top of the list of concerns in cloud computing. It stores the public information, encrypted data and responds to each class access requests. CSP also has its own secret key so that only authorized users can access the cloud storage through CSP.

When the user wants to download the particular file from the cloud storage the same steps are followed in reverse order to download the file from the cloud storage. The user needs to download his/her own data from the cloud server, and authorized users can retrieve the data from the cloud. The file is decrypted using a reverse 128-bit AES algorithm along with a user private key and after downloading the file user can end the process.

V. CONCLUTION

Future employment potential in cloud computing is numerous. In a conventional system, the CSP is always exposed to access structures. Therefore, bad users or hackers can simply access user data and give it to unauthorized people. Consequently, a new model that may offer great protection of user-sensitive data. In this work a hierarchical key assignment schema for a secure user data process on cloud, which includes user authentication with private and public keys. The stored files are encrypted with 128-bit AES encryption and sent along with an encrypted 10-bit alphanumeric key which intern provides zero-knowledge encryption. This work provides security to user’s data on cloud from a third party and unauthorized users. We believe that our proposed work provides authentic user login along with a security key for every login hence providing zero-knowledge encryption for user’s data.

References

[1] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, “Achieving Simple, Secure and Efficient Hierarchical Access Control in Cloud Computing,” *IEEE Trans. Comput.*, vol. 65, no. 7, pp. 2325–2331, 2016, doi: 10.1109/TC.2015.2479609.

[2] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, “Efficient Traceable Authorization Search System for Secure Cloud Storage,” *IEEE Trans. Cloud Comput.*, vol. 8, no. 3, pp. 819–832, 2020, doi: 10.1109/TCC.2018.2820714.

[3] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, “An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1265–1277, 2016, doi: 10.1109/TIFS.2016.2523941.

[4] M. P. Babitha and K. R. R. Babu, “Secure cloud storage using AES encryption,” *Int. Conf. Autom. Control Dyn. Optim. Tech. ICACDOT 2016*, pp. 859–864, 2017, doi: 10.1109/ICACDOT.2016.7877709.

[5] S. Lee, I. Ong, H.-T. Lim, and H.-J. Lee, “Two Factor Authentication for Cloud Computing,” *J. Inf. Commun. Converg. Eng.*, vol. 8, no. 4, pp. 427–432, 2010, doi: 10.6109/jicce.2010.8.4.427.

[6] G. Hu, “Study of file encryption and decryption system using security key,” *ICCET 2010 - 2010 Int. Conf. Comput. Eng. Technol. Proc.*, vol. 7, pp. 121–124, 2010, doi: 10.1109/ICCET.2010.5485326.

[7] R. Luchs and L. Sneeringer, “Zero-Knowledge Encryption in the Cloud : a Solution for,” *Univ. Pittsburgh, Swanson Sch. Eng. 03.02.2018*, 2018.

[8] UKessays, “Internet Source.” https://www.ukessays.com/

[9] Geeksforgeeks, “Internet Source.” https://origin.geeksforgeeks.org/