WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Security in Cloud

Nilesh Kumar

BTech Student, Maharaja Agrasen Institute of Technology,India
Departement of Information Technology

ABSTRACT-

Cloud Computing has been envisioned as the next-generation IT Enterprise architecture. Data is exchanged between the server and the client on the cloud. The importance of high speed in networking cannot be overstated. Cloud security is a hot topic in the IT industry right now. This study article assists in securing data without impacting network layers and safeguarding data from unauthorized incursions into the server. Data is secured in the server based on the users' preferred security approach, ensuring that data is given top priority in terms of security. Cloud computing has been chosen as the next generation of IT enterprise architecture. Unlike traditional IT systems, which keep IT services under strict physical, logical, and people constraints, Cloud Computing distributes application software and databases to massive data centers, where data and service management may be suspect. This one-of-a-kind feature, on the other hand, introduces a slew of new security issues that aren't widely known. This article focuses on the security of cloud data storage and transfer, which has always been a key part of service quality. We propose an effective and flexible distributed scheme with two salient features to ensure the correctness of users' data in the cloud. Unlike its predecessors, cloud storage allows users to remotely store their data and enjoy on-demand high-quality cloud applications without the burden of local hardware and software management. This essay looks at the challenges and answers to establishing a secure cloud computing environment..

Keywords : Encryption, Decryption, Splitting, Sharing, Cloud

INTRODUCTION:

IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) are the three basic types of cloud computing services (Software as a Service). The main difference between a cloud-based service and a typical service is that customer data is kept in the service provider's distributed storage system rather than on the local server. Users (particularly corporate users) have high expectations for data security and reliability in many circumstances. Plaintext data is typically stored after encryption in traditional data protection technologies. Symmetric encryption methods, such as DES and AES, are commonly used in practical applications due to their efficiency. Although the data on the cloud server is encrypted, the encryption algorithm has a lower level of protection. As a result, encrypted data is extremely vulnerable to attacks, and commercial interests are jeopardized once the server is breached. We offer a secure data storage technique in this research that addresses the inadequacies of standard data protection methods while also boosting cloud computing security and reliability.

1.1 Cloud Computing

Cloud computing, like a utility (such as the power grid) through a network, relies on resource sharing to achieve coherence and economies of scale. The wider concept of integrated infrastructure and shared services lies at the heart of cloud computing.

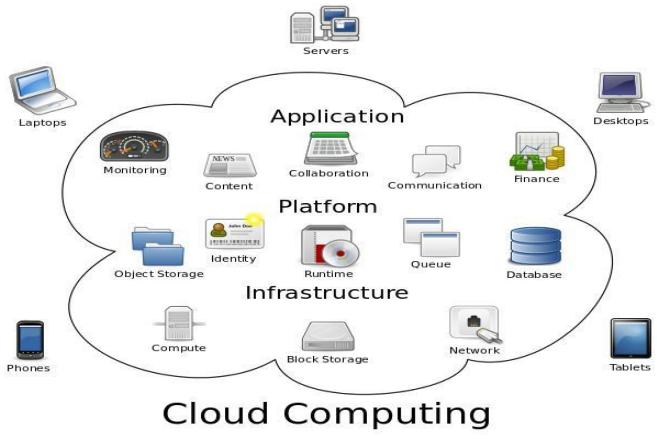


Fig 1.1 Cloud computing metaphor

Cloud computing, or simply "the cloud," is likewise concerned with increasing the efficiency of shared resources. This method can be used to allocate resources to users. For example, a cloud computer facility that serves European users with a specific application (e.g., email) during European business hours may reallocate the same resources to serve North American users with a different application during North American business hours (e.g., a web server). Because less power, air conditioning, rack space, and other resources are required for a variety of operations, this strategy should maximize the use of computer power while also reducing environmental damage. Various users can use a single server to receive and update their data using cloud computing, which eliminates the need for multiple licenses for different applications.

METHODOLOGY

1.1 DES (Data Encryption Standard)

The data encryption standard (DES) is a widely used data encryption standard and a type of secret key cryptography (SKC) that encrypts and decrypts data using only one key. PKC (public key cryptography) employs two keys: one for encryption and the other for decryption.
.DES is a block cipher, which takes a fixed-length string of plaintext bits and transforms it into another ciphertext bit string of the same length using a series of sophisticated operations. The block size in the case of DES is 64 bits. DES also employs a key to modify the transformation, implying that decryption can only be accomplished by those who have access to the encrypting key. The key is supposed to be 64 bits long, but only 56 of them are utilised by the algorithm. Eight bits are utilized simply for parity verification and then deleted. As a result, the effective key length is always stated as 56 bits.

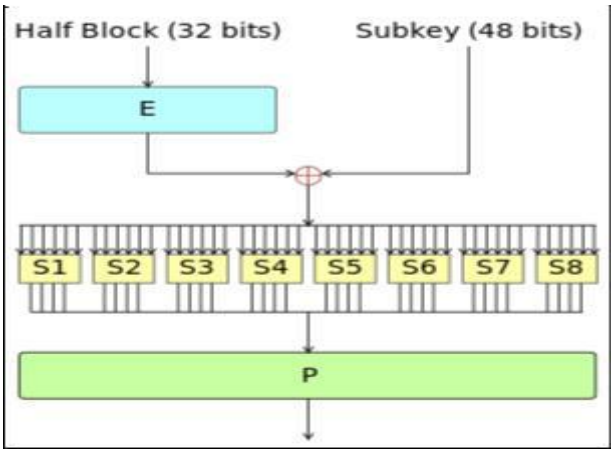


Fig 1.2 The Feistel function (F function) of DES

1.2-XML

The Extensible Markup Language (XML) is a markup language that specifies a set of rules for encoding documents in a human- and machine-readable format. XML's design goals stress simplicity, universality, and usability across multiple platforms.

the World Wide Web It's a textual data format with robust Unicode compatibility for a variety of human languages. Although XML was created with the intent of representing documents, it is now commonly used to represent arbitrary data structures such as those found in web services. Many office productivity programs, including Microsoft, now use XML-based formats as their default.

1.3-.NET

Net was created with the goal of making it simple for skilled programmers to learn and utilize. The model of the thing. Simple types, such as integers, are preserved as high-performance non-objects, making Net simple and straightforward to modify.

Because a program must run consistently on a range of systems, the web's multiplatform environment throws extraordinary demands on it. As a result, the ability to write strong applications was prioritized in the development of.Net. At the same time,.Net relieves us of the burden of dealing with many of the most typical causes of programming errors. Because.Net is a strongly typed language, it verifies our code both at build and runtime.

The Internet was created to satisfy the real-world needs of providing interactive, multimedia content.

IMPLEMENTATION

2.1 Module Description

2.1.1 Login Module

A login, logon, or sign in is a term used in computer security to describe the credentials required to gain access to a computer system or other restricted area. Individual access to a computer system is regulated by identifying and authenticating the user through the credentials given by the user by logging in or on and signing in or on.

After logging in, a person can log out or log out when their access is no longer required. After previously logging in, to log out means to close one's access to a computer system.

2.1.2 Registration Module

Obtain a username, email address, and password upon registration, and have the user produce a random verification code. A new random number generator. To produce random code, use Next(). The user can log in and move on to the next step, which is the verification code. SMTP protocol is used to send email to the user's email address. If the verification code is blank, the user is redirected to the login page; if the code matches, the user's status field is updated with the text active, and the user is redirected to the home page.

2.1.3 FTP Setting Module

Files are dispersed at three separate locations in the proposed system. The first site is our application, followed by two more FTP locations for the second and third files. We develop a setup page in the suggested system, which will be utilized by the program to upload and download files from the established table. FTP details should be entered into the table.

2.1.4 Upload and Download module

Create a web interface that allows users to upload and download files from cloud storage. The various file uploading links are active. The user can choose which link to upload to the cloud. The user can upload any type of content to the cloud, including docs, videos, and mp3s. The homepage will display a list of files that the user has uploaded from a user-defined directory. In the proposed system, we employ a data list to display a file list file class that allows us to retrieve folder and file details such as file name and size. We may allow the user choose which file to upload by using the file uploader control. Using Server, you may get the server path. To acquire the path of the server directory, use the Map Path () function.

2.1.5 File encryption technique module

Encryption is the process of encrypting messages or information so that only authorized parties can read it in cryptography. Encryption does not prevent interception in and of itself, but it does deny the interceptor access to the communication content. The plaintext of a message or piece of information is encrypted using an encryption method, resulting in ciphertext that can only be read if decrypted. An encryption technique commonly employs a pseudo-random encryption key generated by an algorithm for technical reasons. Although it is theoretically possible to decrypt a communication without knowing the key, a well-designed encryption scheme necessitates a lot of processing power and expertise. With the key provided by the originator to recipients, an authorized recipient can simply decode the message, but not unauthorized interceptors. Setting up and configuring several cloud servers in order to gain access to cloud storage. Each one has its own cloud server. Before storing files in the cloud, developing encryption techniques such as RSA, AES, and DES for file decryption. For encryption and file splitting, we use a combination of AES and SHA-1 algorithms in the proposed system.

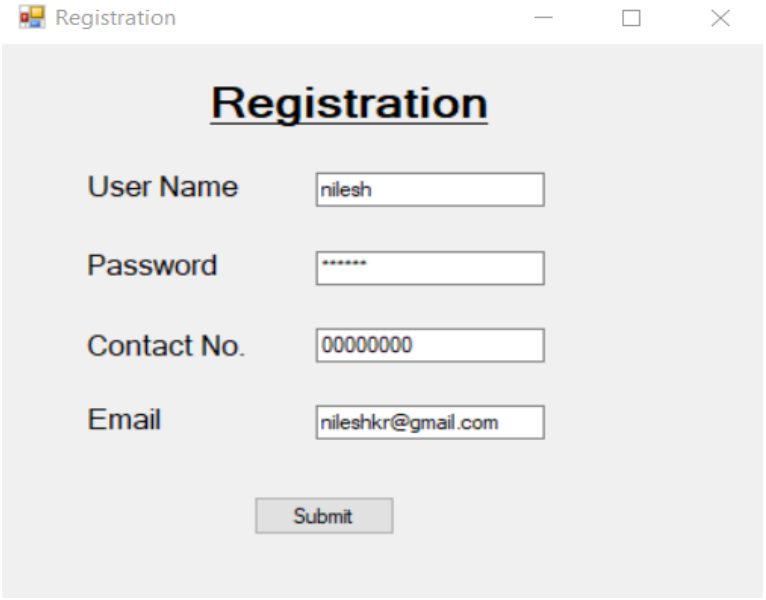
2.1.6 File decryption technique module

Decryption is the process of transforming encoded or encrypted text or other data back into text that you or your computer can comprehend. This phrase can be used to indicate a way of manually decrypting data or a method of decrypting data using the correct codes or keys. It's possible that data will be encrypted to make it more difficult for someone to steal it. Encryption is also used by some firms to protect company data and trade secrets in general. If the data needs to be viewed, decryption may be required. If a decryption passcode or key is not accessible, special software to crack the decryption and make the data readable may be required.

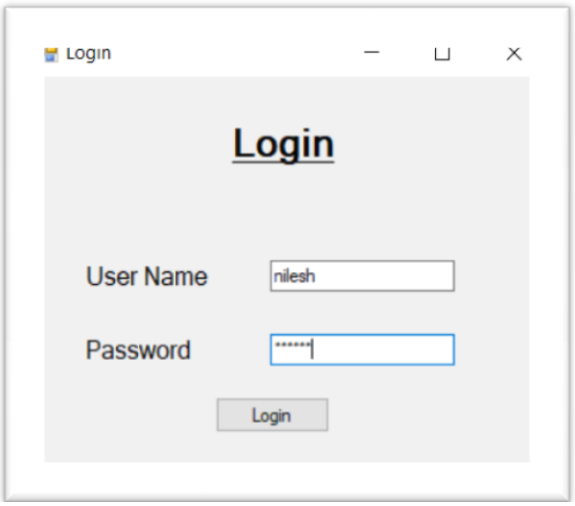
2.1.7 File splitting and clubbing module

We partition the file into distinct pieces in the proposed method, then encode and store it on different clouds. The metadata management server will keep the meta data required for decrypting and transferring a file. A file can join forces with another file.

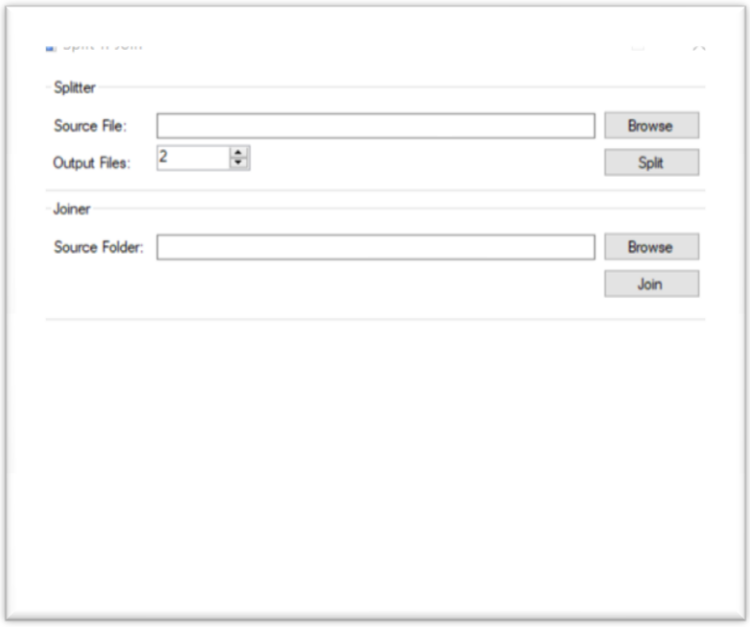
Home Page



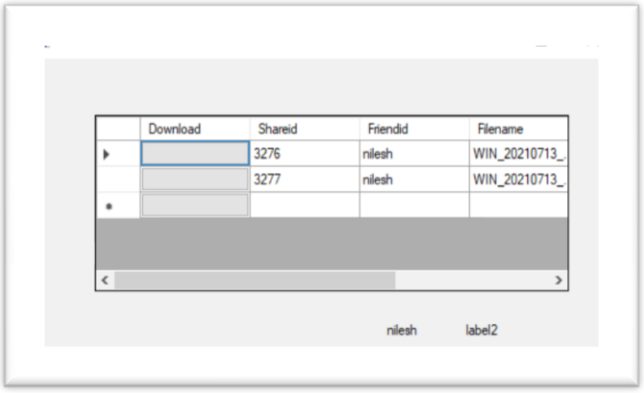
Registration Page



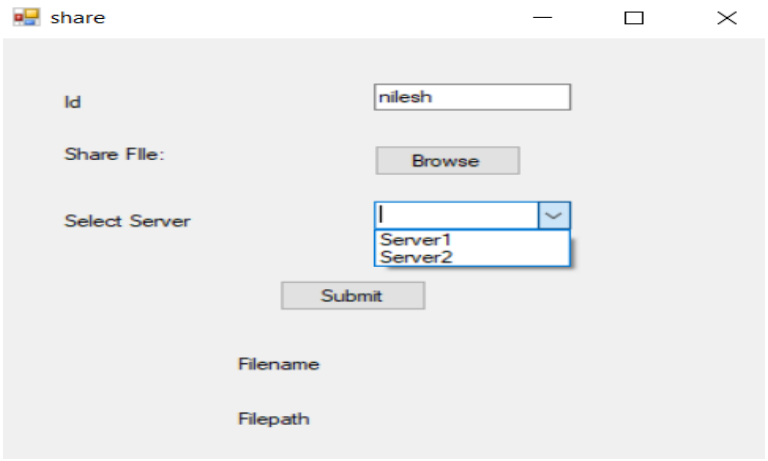
Login Page



Split and Join Page



Download Page



Share Page

CONCLUSION

Users keep their data in the cloud, therefore there is no need to store it locally, as noted in the cloud data storage system. As a result, data files on storage distributed cloud servers are guaranteed in terms of security, integrity, and availability. To do so, researchers should look into the structure and security solutions of the various parts involved in the data storage process in the cloud. Regarding the first piece, client, we recommend using a customer-provided encryption mechanism such as DES encryption, which has been demonstrated to be highly secure and resistant in several tests. We can also integrate encryption algorithms with new approaches such as genetic algorithms or other dynamic algorithms, resulting in a significant gain in security. Because our data is stored on the server and we have virtual storage space as users, the next element must pay special attention to its security. As a result, data and information retrieval accuracy and availability are critical, and the server should provide the necessary security to accomplish this. As a result, we used a comparison of some security policies by well-known providers of data storage services. From the comparison, it is obvious that some providers use encryption control mechanisms such as symmetric encryption to ensure information confidentiality. Regarding the security of our server, we advise service providers in this field to expand and improve security mechanisms on their servers, as users of cloud technology will gravitate toward those providers whose services are sufficiently secure. As a result, server security will be important, and providers will be able to succeed in this technology if their servers are secure and accountable to their users.

The connection channel between cloud service providers and users is the third element whose security is critical in the storage and transfer of data. Communication channels, in our opinion, are the most susceptible area in the cloud environment that might jeopardize user data and information. Because of the Internet and, in most cases, outdated systems, we must employ new techniques to prevent illegal effects. In this case, we're talking about existing protocols and retrieving or constructing more secure communication channels that they introduce by employing new computer science techniques and methodologies.

FUTURE SCOPE

With the following modifications, the HRMS can be evolved into a separate, automated system for managing the process:

It is possible to include a help file. As of present, the system does not provide any kind of assistance to its users. With a special function key and help command on the main page, a help menu can be created. Help can be displayed in a separate window, as a link to a printed manual, or as a one- or two-line recommendation in a fixed screen location.

Typed commands can be used by the system, as they were once the most prevalent mode of communication. Control sequences, function keys, or typed words can all be used to send a typed command.

The system can incorporate a training element. This module can be used to educate system users on how to use the system.

REFERENCES

[1] Pradnyesh Bhisikar, Prof. Amit Sahu , ―Security in Data Storage and Transmission in Cloud Computing‖, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 3, Issue 3, March 2013, ISSN: 2277 128X.

[2] Security and Privacy Challenges in Cloud Computing Environments‖ co-published by the IEEE computer and reliability ieee November/december 2010

[3] Sameera Abdulrahman Almulla, Chan Yeob Yeun, ―Cloud Computing Security Management,‖ Engineering systems management and its applications (2010), pp. 1-7.

[4] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, ―Cloud Computing: A Practical

[5] K. inzhu, "A Practical Approach to Improve the Data Privacy of Virtual Machines," in Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, 2010, pp. 936-941..

[6] Z. Xiao, D. Hong-tao, C. Jian-quan, L. Yi, and Z. Lei-jie, "Ensure Data Security in Cloud Storage," in Network Computing and Information Security (NCIS), 2011 International Conference on, pp. 284-287.

[7]K. S. Sandeep, "A combined approach to ensure data security in cloud computing," J. Netw. Comput. Appl., vol. 35, no. 6, pp. 1831-1838

[8]W. Jian, Z. Yan, J. Shuo, and L. Jiajin, "Providing privacy preserving in cloud computing," in International Conference on Test and Measurement, (ICTM '09) 2009, pp. 213-216.

[9]R. Ranchal, B. Bhargava, L. B. Othmane, L. Lilien, K. Anya, K. Myong, and M. Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party," in Reliable Distributed Systems, 2010 29th IEEE Symposium on, pp. 368-372.

[10] Shah Kruti R., Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[11] Shasi Mehlrotra seth, Rajan Mishra,―Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011.

[12]B. Shwetha Bindu, B. Yadaiah, ―Secure Data Storage In Cloud Computing‖, International Journal of Research in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.

[13] Ravi Gharshi, Suresha, ―Enhancing Security in Cloud Storage using DES Algorithm‖,International Journal of Science and Research (IJSR), Vol 2, Issue 7, 2013