



ENHANCING SECURITY IN CLOUD USING STEGNOGRAPHY AND CRYPTOGRAPHY

Nilesh Kumar

Department of Information Technology B Tech Student, Maharaja Agrasen Institute of Technology, India

ABSTRACT:

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In the cloud, the data is transferred among the server and client. High speed is the important issue in networking. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the network layers and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority. Cloud Computing has been selected as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage and transmission security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors, cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. This article explores the barriers and solutions to providing a trustworthy cloud computing environment. consequences.

Keywords: Encryption, Decryption, Splitting, Sharing, Cloud

Introduction:

Cloud computing mainly provides three kinds of services: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The major difference between service based on cloud computing and traditional service is that user data is stored not in the local server, but in the distributed storage system of the service supplier. In many cases, however, users (especially business users) have high demands regarding data security and reliability. Generally, in traditional data protection methods, plaintext data is stored after encryption. In practical applications, symmetric encryption algorithms, such as DES and AES, are usually adopted because of their efficiency. Although data stored in the cloud server are encrypted, encryption algorithm provides relatively lower security. Therefore, encrypted data are very likely to be vulnerable to attacks and business interests become compromised once the server is invaded. In this project, we propose a secure data storage strategy capable of addressing the shortcomings of traditional data protection methods and improving security and reliability in cloud computing.

1.1 Cloud Computing

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

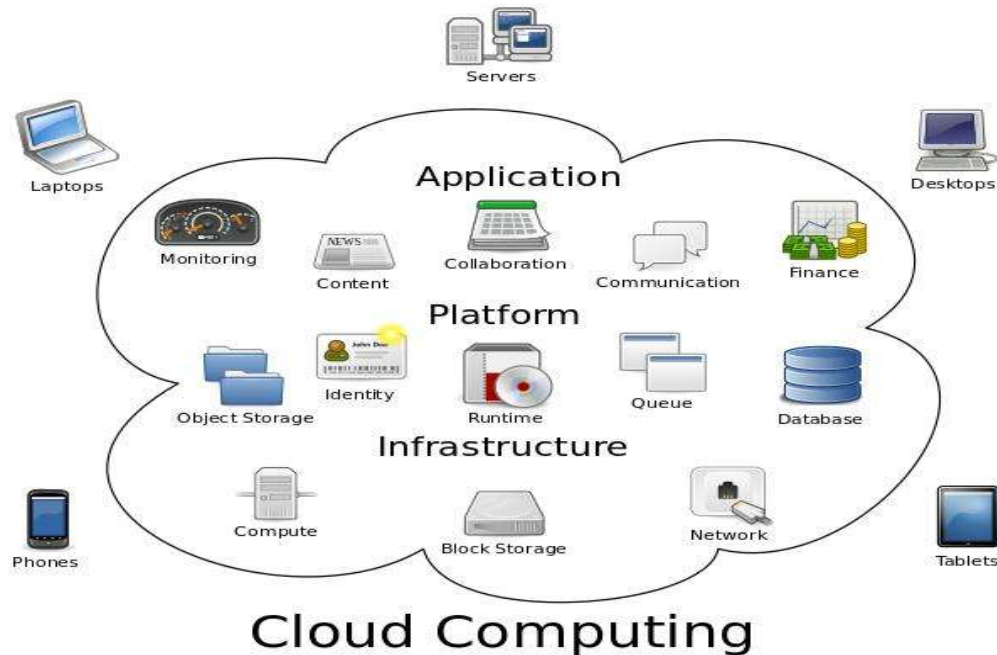


Fig 1.1 Cloud computing metaphor

METHODOLOGY

1.1 DES (Data Encryption Standard)

The data encryption standard (DES) is a common standard for data encryption and a form of secret key cryptography (SKC), which uses only one key for encryption and decryption. Public key cryptography (PKC) uses two keys, i.e., one for encryption and one for decryption.

DES is a block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such.

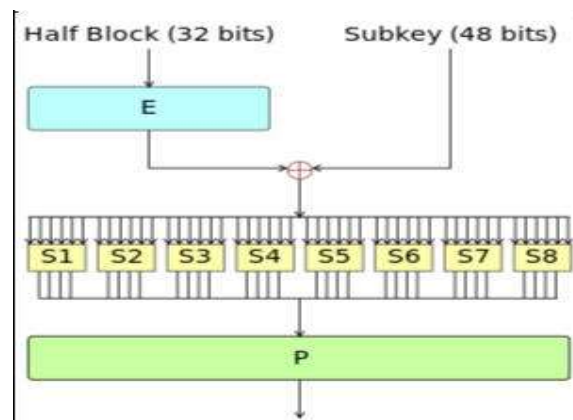


Fig 1.2 The Feistel function (F function) of DES

1.2-XML

Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable. The design goals of XML emphasize simplicity, generality and usability across the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures such as those used in web services. XML-based formats have become the default for many office-productivity tools, including Microsoft.

1.3-.NET

Net was designed to be easy for the professional programmers to learn and use efficiently. The object model of .Net is simple and easy to extend, while simple types, such as integers are kept as high-performance non-objects.

The multiplatform environment of the web places extraordinarily demands on a program, because the program must execute reliably in a variety of systems. Thus, the ability to create robust programs was given a high priority in the design of .Net. At the same time, .Net frees us from having to worry about many of the most common cause of programming errors. Because .Net is strictly typed language, it checks our code at the compile time and also at run-time.

Net was designed to meet the real world requirements of creating interactive,

IMPLEMENTATION

2.1 Module Description

2.1.1 Login Module

In computer security, a login or logon or sign in refers to the credentials required to obtain access to a computer system or other restricted area. Logging in or on and signing in or on is the process by which individual access to a computer system is controlled by identifying and authenticating the user through the credentials presented by the user.

Once a user has logged in, they can then log out or log off when access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

2.1.2 Registration Module

In registration get username, email address, password, user generate random verification code. New Random. Next () is used to generate random code. The user can sign in and proceed to next step to verification code. Mail is to user email address by using SMTP protocol. The user can verify the code if verification code is blank then redirect to login page else matched then update user status field with text active and redirect user to the home page.

2.1.3 FTP Setting Module

The proposed system, file get distributed at three different location. First location that is our application and next two more FTP where 2nd and 3rd file is store. In proposed system, we design setting page where this will be further used by application to upload and download file from created table. Insert into table FTP details.

2.1.4 Upload and Download module

Develop a web interface to upload and download files in cloud storage. The different file uploading links are open. The user can choose the link which we want to upload on cloud. User can upload the file on cloud such as doc file, video, mp3, etc. Homepage will show list of file uploaded by user from user specific directory. In proposed system, we use data list to show file list file class to get folder and file details like file name, file size. Upload file by using file uploader control we can let the user select file to be upload. Get the sever path by using Server. Map Path () function to get path of server directory.

2.1.5 File encryption technique module

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. Setting up and configuring different cloud server in order to having storage cloud access. Each clouds its own server. Developing encryption technique like RSA, AES, DES for file decryption before storing it on cloud. In proposed system, we use combination of AES algorithm and SHA-1 algorithm for encryption and splitting of File.

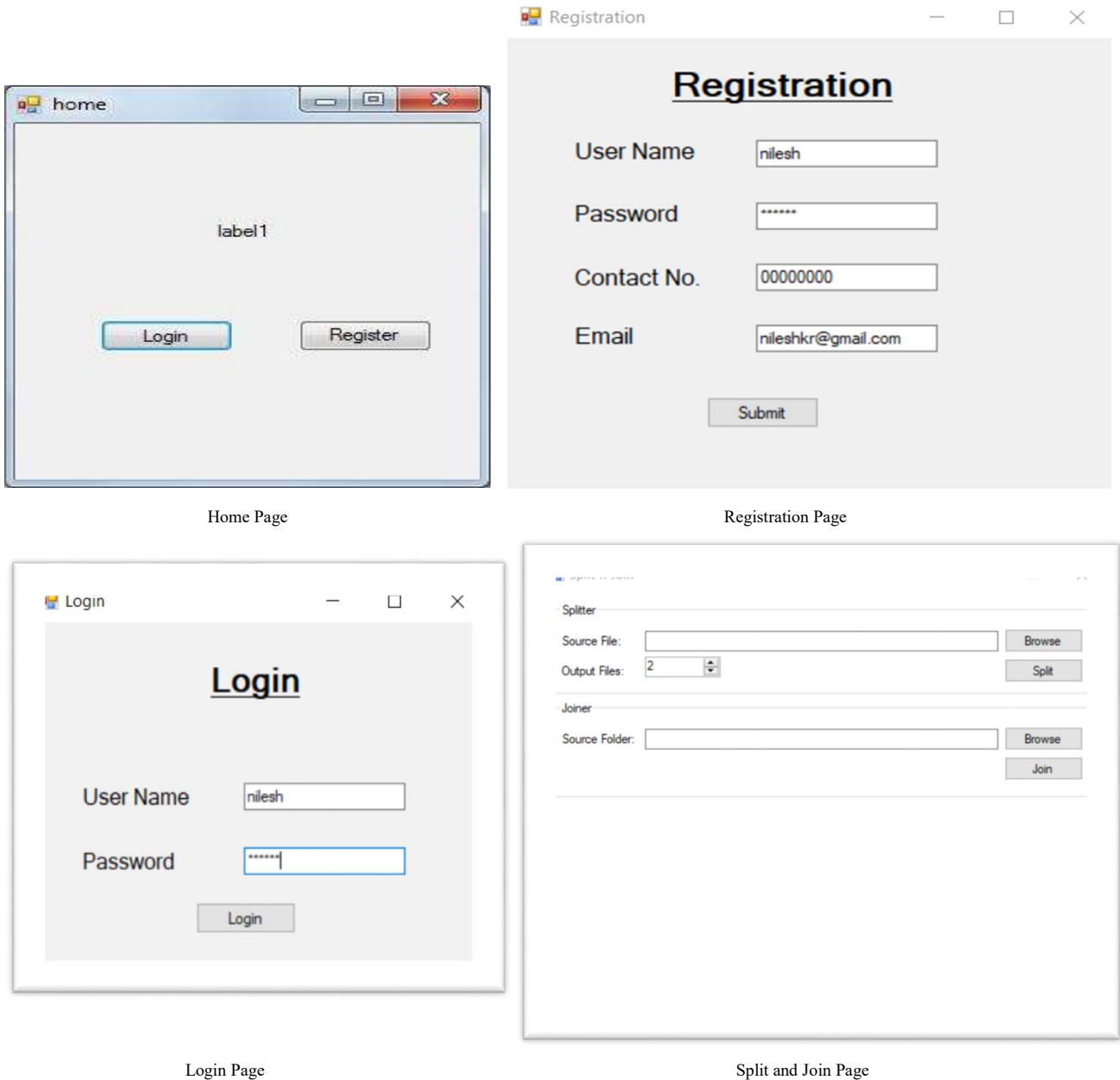
2.1.6 File decryption technique module

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of

company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

2.1.7 File splitting and clubbing module

In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

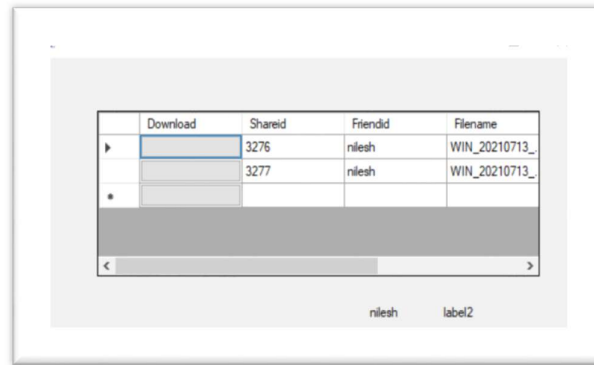


Home Page

Registration Page

Login Page

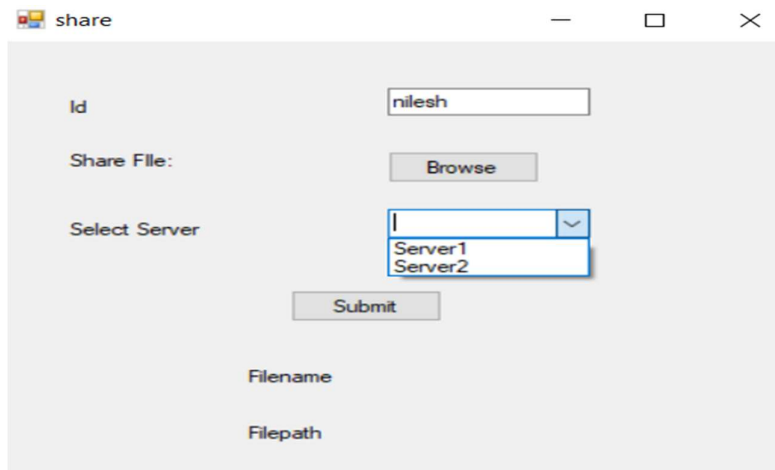
Split and Join Page



Download	Shareid	Friendid	Filename
	3276	nilesh	WIN_20210713_
	3277	nilesh	WIN_20210713_

nilesh label2

Download Page



share

Id: nilesh

Share File: Browse

Select Server: Server1, Server2

Submit

Filename

Filepath

Share Page

CONCLUSION:

As noted in the system of cloud data storage, users store their data in the cloud, so there is no need to store them locally. Therefore, the security, integrity and availability of data files on storage distributed cloud servers are guaranteed. To accomplish this, the structure and security solutions of involved elements in the process of data storage in the cloud environment should be investigated. About the first element: client; we suggest to use an encryption mechanism from the customer like DES encryption that its high security and resistance has been proven in many testing. Also we can use encryption algorithm by means of new methods like genetic algorithm or other dynamic algorithm which security can increase dramatically in this way. The next element must give special consideration to its security is server, because our data store on the server and we possess storage space virtually as a user. Therefore, the accuracy and availability of data and information retrieval is very important and should provide the necessary security to accomplish this on the server side. Therefore, we use a comparison between some security policies by providers known in the field of providing data storage services, we did the comparison can be clearly seen that in order to the confidentiality of information, some providers use the mechanism of encryption control such as symmetric encryption. About the security of our server recommended service providers in this field to expand and to improve security mechanisms on their servers, because the users of cloud technology will go to the side of those providers that their services have enough security, thus server security will be important and providers can success in this technology with high server security and accountability to the users.

The third element that its security is important in the storage and transmission of data is the connection channel between cloud service providers and user. In our opinion, the most vulnerable point that can put user's data and information in the cloud environment at risk are communication channel. Because of the Internet and in most cases of the old mechanisms, therefore we must use new methods in order to avoid of unauthorized influences. In this case we can refer to the established protocols and retrieving or establishing more secure transmission channels that they introduce by using new sciences and methods in the computer science.

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 Mehlotra 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