JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY ENHANCEMENT OF DATA ON CLOUD USING LSB TECHNIQUE AND SPLITTING TECHNIQUE

Versha (Student)
Department of Computer Science
D.P.G. Institute of Technology and Management, Gurgaon 122001
Gurgaon, India
Vershayadav327@gmail.com

Dr Sonal Kanungo (Guide)
Department of Computer Science
D.P.G. Institute of Technology and Management, Gurgaon 122001
Gurgaon, India
Drsonal.cse@dpgitm.com

Mr.Yash Dhankhar(Co-Guide)
Department of Computer Science
D.P.G. Institute of Technology and Management, Gurgaon 122001
Gurgaon, India
yashdhankhardpgitm@gmail.com

ABSTRACT:-Security is vital for sharing sensitive information in the cloud. Using the genuine key performs the structure share the fragile information without moving Keys for every record. This structure occupations Hilter kilter encryption standard for encrypting all the information is trailed by open key encryption. The clients will get their information recovered once they put the private key and a public key they got from the sender. If the key is hacked during transmission, the suspect attacker won't get the information to decode as the private key gets the information. It isn't obligatory to share keys for each document since they can decrypt the record utilizing a private key. The special secret key concentrates all data and information. So the information is secured in better places, and clients can use it anywhere.

Keywords: ***Cloudsecurity, Data on cloud, cloud data***

I. INTRODUCTION

Over the few years, the demand for cloud computing is very high, leading to the innovation of new techniques and security concerns. Still, the biggest problem of cloud servers is security. Due to security concerns of the cloud, much research has been done which enhance security. Besides the security challenges, cloud architecture has many new advances and unique features that expose the route in techniques, approaches and safety.

Our research suggested the new data security approach and reviewed the previous work done in the cloud security area. Much other technique and security architecture has been discussed. Our research will try to overcome the issue and explain cloud computing and its benefits in the business.

Provisioned as a service over the internet, the cloud offers scalable and dynamic resources. Services provided by cloud infrastructures like third party, on-demand, self-service and self-management, pay per use is the model which helps to reduce the operational and capital expenses for software and hardware for the users.

Normally, ensure that a solid framework track across different PCs implies parting the record into customer and server modules. As computers proliferated, dropped in cost, and became connected by ever-higher

bandwidth networks, splitting software systems into multiple components became more convenient, with each component running on a different computer and performing a specialized function.
The server handles the user records like printing, logs etc., whereas the client module handles the user interface in such a system. The failure of one system in the cluster does not affect the other system since the approach analysed management, administration and development, which improve the performance.
In our proposed system, we are using the concept of a multi-storage cloud system, which enhance the security of each file using the splitting technique. And each part has been encrypted with an AES encryption algorithm. After encrypting each file, we would upload the part files to different cloud servers.

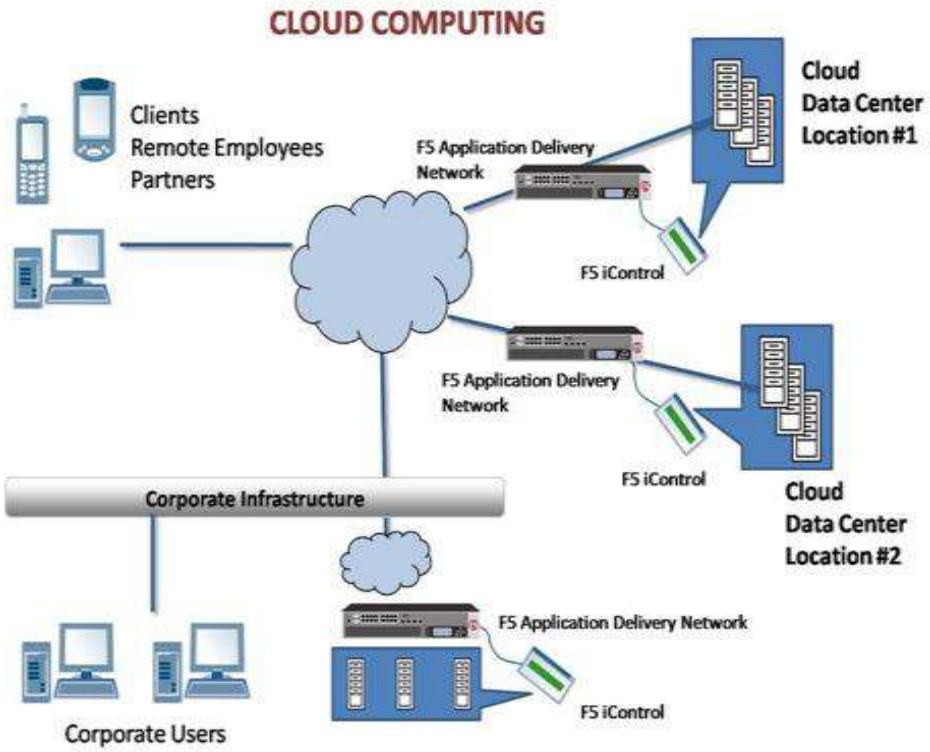

Figure 1: Cloud computingarchitecture

II. REASERCH METHODOLOGY

Step 1: Signup

In the signup module, the User has to enter his name, email, contact and password. Once the data has been entered, our program validates the user input. If the validation is successful, user input data is stored in the database. If the data entered by the User is not valid, it shows a validation error.

Step 2: Steganography

In this module, the user selects the image in which he has to hide the plain text. Once the user selects the image, he inserts the plain text.Once the user is done with these processes, it will show the user an alert message to save the image once the image has been saved. The plain text gets encrypted to the picture.

Step 3: File split and join module

We split the file into different parts in the Proposed System. In this technique, the user has to choose the steganography image to split. Once the image is split, it gets stored in the destination location with the '.part' extension when the user joins the split files. Our program looks for the '.part' extension and gets merged and saved in the desired format, whatever the user wants to save the file.

Step 4: File encryption technique module

In this module, we use the AES encryption technique to encrypt the files.The user has to choose the split files for encryption; once the user selects the file to encrypt, our program asks where to store the file. Once the user selects the location, the file gets stored in the destination with the '.enc' extension.

Step 5: File compression

In this module, the user has to choose the folder in which they have stored the encrypted file and the click on zip button; once the zip button is clicked, the Gzipstream algorithm is applied, which zipped all the files in the folder.

Step 6: Upload and Download module

Develop an interface to transfer the files on the server and download them once the Uploader uploads the files and enter the name of the receiver party. The receiver gets a notification then someone shared a file. Now, the receiver can download the file when the receiver clicks on the download file button. The files get downloaded to E drive by default.

Advantages:

- Provide security
- Provide multilayer upload and secure files

III. SPLIT TECHNIQUE

In our proposed system, we ask for the user to choose the file they want to split. Once the file has been chosen. Our program asks for the number of parts he wants to split the file and the location they wants to save. Once the number is chosen, then the user will click on split button, then the file gets splitted. Once the file gets spitted, the file gets stored in the selected destination. The splitted file stored with filename and '.part' extension.

In merge section, User has to choose the destination folder where they kept splitted files. Once the user choose the splitted files folder, our program ask for the desire location where the user wants to save the merged files, Once the user selected the destination location and he extension and clicked on merge button, our program start searching only the '.part' extension files. Our file gets merged and stored in the selected location.The Split is done through the following steps

Step 1: Start.
Step 2: Choose file.
Step 3: Choose the location.
Step 4: Split the file into n parts.
Step 5: Store the file in the selected location.
Step 6: Stop

Merge Technique works in the following ways

Step 1: Choose Splitted files folder
Step 2: Choose the location and extension
Step 3: Merge the files.
Step 4: Store the file in the selected location
Step 5: Stop

5.5 Encryption

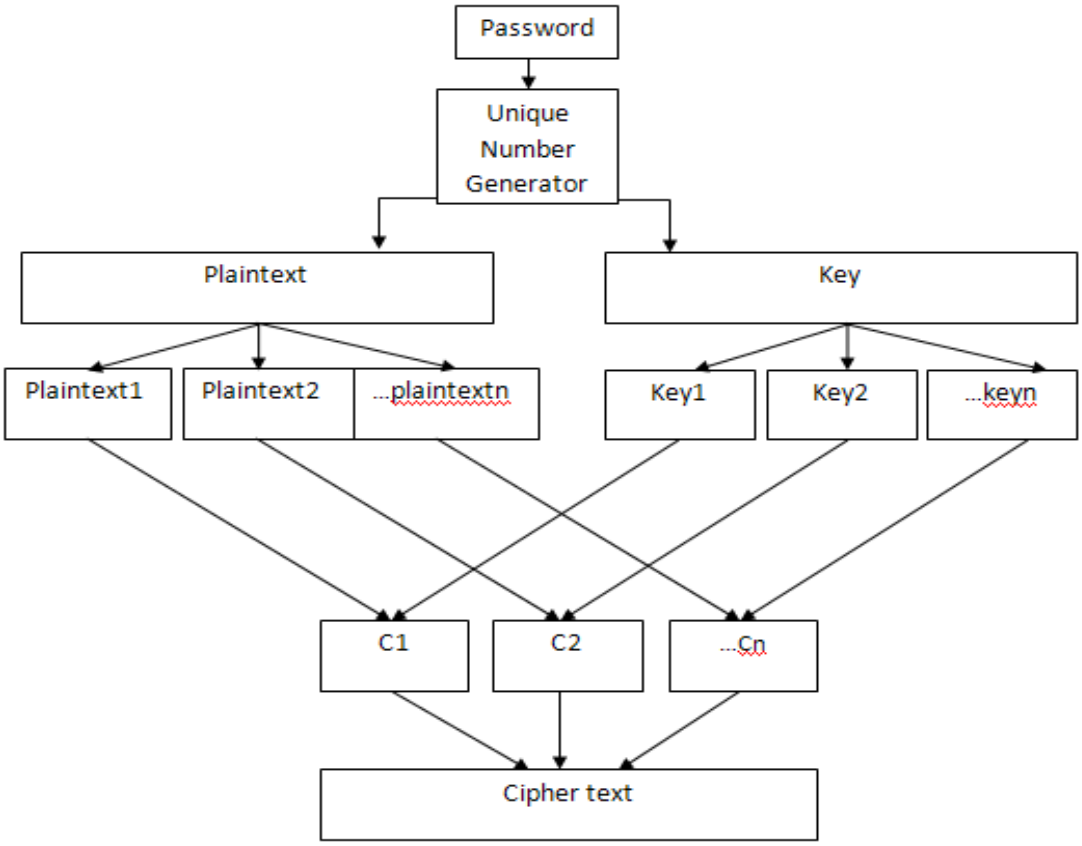

Figure 2: Encryption

Flowchart – Decryption

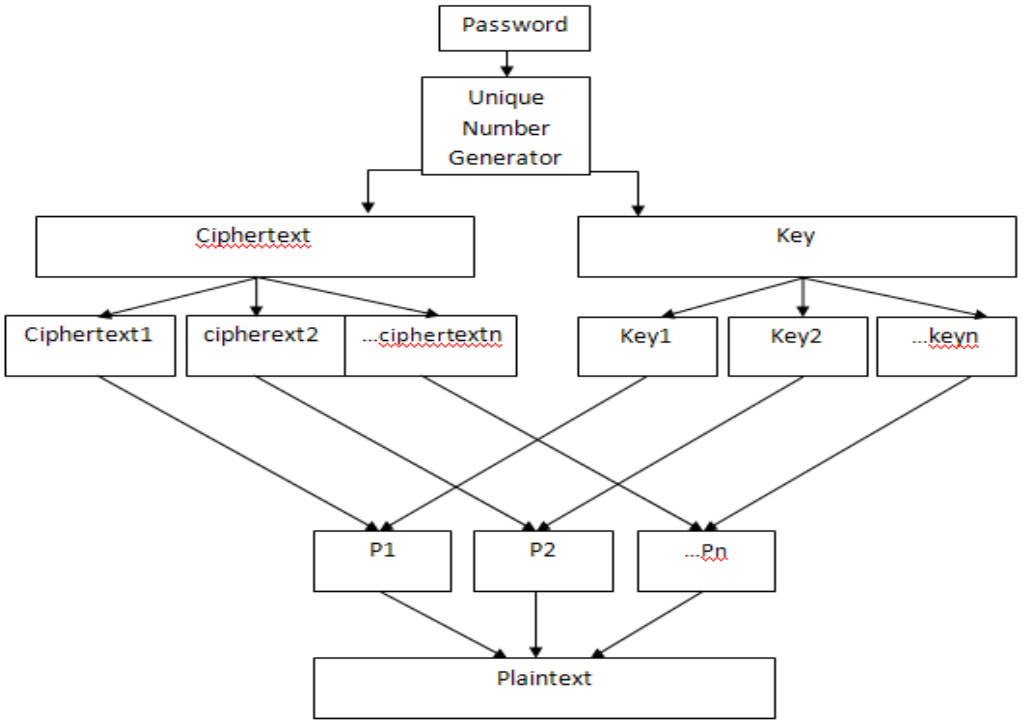

Figure 3: Split-file -key pair algorithm –Decryption

IV. SIMULATION RESULT

LOGIN

Fig 4: Login it if you have already register

SPILT AND JOIN

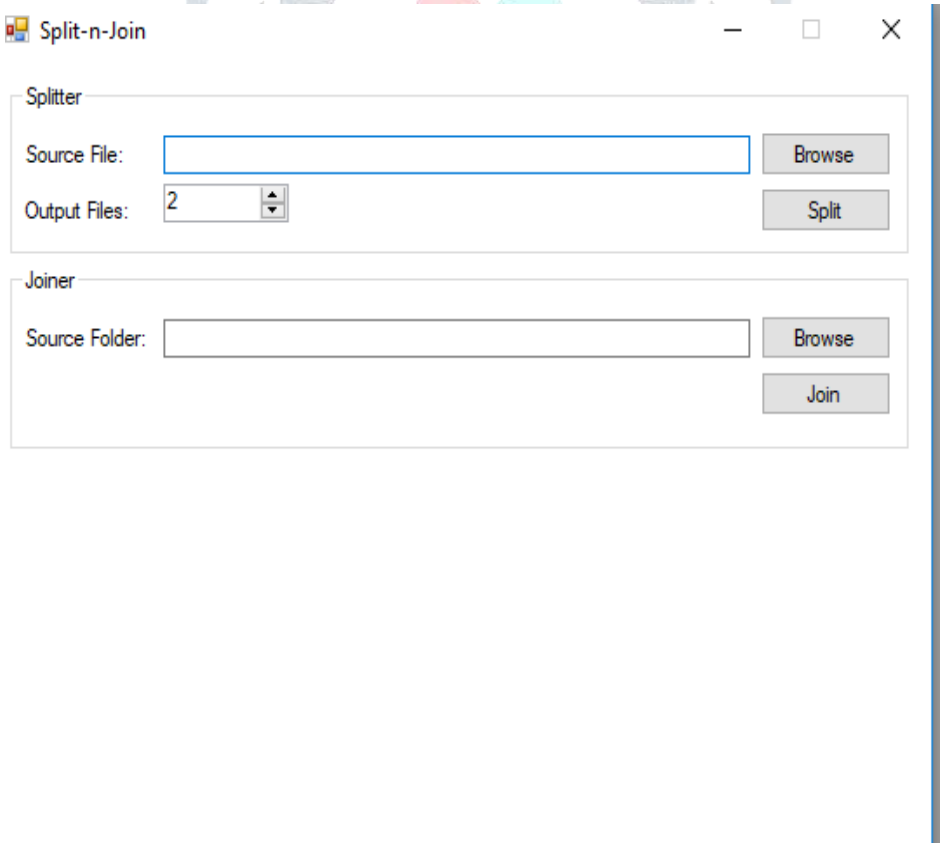

Fig 5: Go to Multimedia Option, then Split and join a file

ENCRYPT AND DECRYPT

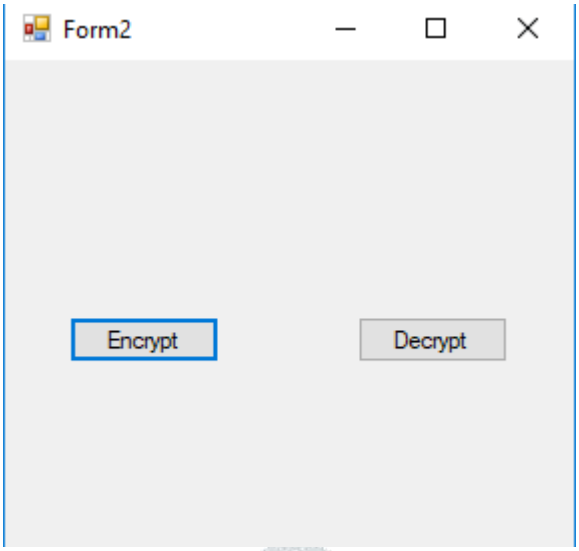

Fig 6: Form for encrypt and decrypt

V. CONCLUSION

It tackles numerous business secure and safe storage issues by performing cloud-based storage. Yet, on the opposite side, numerous scholars express that it is more dangerous to put the information over a single cloud as it expands the opponent client assault prospects; consequently, by planning the proposed framework, we broaden the capacity of cloud security by dispersing and encoding the information. An online interface that allows the client to deal with his knowledge and the oversaw information ought to be splitter over the numerous cloud drive as a piece of the document and encryption. The proposed framework will be tried and show over a nearby organization or on a live stockpiling cloud worker.

Our association with the Multicloud climate using encryption and part strategy is astonishing. We are going after additional functionalities and oddities to make it essentially more appropriate for cloud structure advancement.

References

[1] L. Grandinetti, O. Pisacane, M. Sheikhalishahi, "Pervasive CloudComputing Technologies: Future Outlooks and InterdisciplinaryPerspectives", IGI Publication, Advances in Systems Analysis,Software Engineering, and High Performance Computing, ISBN-13:978-1466646834, 2013

[2] G.R. Vijay, A.R.M. Reddy, "Investigational Analysis of SecurityMeasures Effectiveness in Cloud Computing: A Study", ComputerEngineering and Intelligent Systems, Vol.5, No.7, 2014.

[3] P. Mell, T. Grance, "The NIST Definition of Cloud ComputingRecommendations of the National Institute of Standards andTechnology", Special Publication, pp. 800-145, 2011.

[4] A. J. Adoga, G. M. Rabiu, A. A. Audu, "Criteria for Choosing AnEffective Cloud Storage Provider", International Journal ofComputational Engineering Research, Vol.04, Iss.2, 2014

[5] R.A. Popa., J.R. Lorch., D. Molnar., H.J. Wang., and L. Zhuang.,"Enabling Security in Cloud Storage SLAs with Cloud Proof", InUSENIX Annual Technical Conference, Vol. 242, 2011.

[6] Y. Tang., P.P.C Lee., J.C.S Lui., and R. Perlman., "FADE: Secureoverlay cloud storage with file assured deletion", In Security andPrivacy in Communication Networks, Springer Berlin Heidelberg, pp.380-397, 2010.

[7] W. Ren., L. Yu., R. Gao., F. Xiong., "Lightweight andCompromise Resilient Storage Outsourcing with Distributed SecureAccessibility in Mobile Cloud Computing", TSINGHUA Science andTechnology, Vol. 16, No. 5, pp. 520-528, 2011.

[8] X. Dong., R. Li., H. He., W. Zhou., Z. Xue., and H. Wu., "SecureSensitive Data Sharing on a Big Data Platform", TSINGHUA Scienceand Technology, Vol. 20, No. 1, pp. 72-80, 2015.
[9] A. Bessani., M. Correia., B. Quaresma., F. Andre, and P. Sousa.,"DepSky: dependable and secure storage in a cloud-of-clouds", ACMTransactions on Storage (TOS), Vol. 9, No. 4, 2013.
[10] J. Stanek., A. Sorniotti., E. Androulaki., and L. Kencl., "A securedata deduplication scheme for cloud storage", In FinancialCryptography and Data Security Springer Berlin Heidelberg, pp. 99-118, 2014.
[11] B.H. Kim., W. Huang., and D. Lie., "Unity: secure and durablepersonal cloud storage", In Proceedings of the 2012 ACM Workshopon Cloud computing security workshop, pp. 31-36, 2012.
[12] N. Cao., S. Yu., Z. Yang., W. Lou., and Y. T. Hou., "Lt codesbasedsecure and reliable cloud storage service", In INFOCOM,Proceedings IEEE, pp. 693-701, 2012.
[13] S.Murthy., "Cryptographic Secure Cloud Storage Model withAnonymous Authentication and Automatic File Recovery", ICTACTJournal on Soft Computing, Vol. 5, No. 1, 2014.
[14] H. Xiong., X. Zhang., D. Yao., X. Wu., and Y. Wen., "Towardsend-to-end secure content storage and delivery with public cloud", InProceedings of the second ACM conference on Data and ApplicationSecurity and Privacy, pp. 257-266, 2012.
[15] P. Gasti., G. Ateniese., and M. Blanton., "Deniable cloud storage:sharing files via public-key deniability", In Proceedings of the 9thannual ACM workshop on Privacy in the electronic society, ACM, pp.31-42, 2010.
[16] S. Kamara., C. Papamanthou., and T.Roeder, "Cs2: A searchablecryptographic cloud storage system", Microsoft Research, TechReport MSR-TR, Vol.58, 2011.