E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

"SECURE FILE HOSTING"
A PERFECT SOLUTION ON INFRASTRUCTURE AS SERVICE

[1]Vaibhav M. Hatwar, [2]Vaibhav S. Wankhede, [3]Prof.Kaustubh S. Satpute
[1, 2, 3]*Department of (C.S.E)*
[1, 2, 3]*Datta Meghe College of Engineering, Wardha*
[1] vaibhavh4hatwar@gmail.com, [2,]vaibhavwankhede.135@gmail.com, [3]kaustubh2008satpute@yahoo.com

Abstract— As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system. This model is already quite common for consumer apps like email and photo sharing, and for certain business applications. In this paper we present a way to secure the data using different compression and encryption algorithms and to hide its location from the users that stores and retrieves it. The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which paper is presented is a application based system like which will run on the clients own system. This application will allow users to upload file of different formats with security features including Encryption and Compression. The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the WWW.

Index Terms— Encryption, Decryption, Compression, Decompression, File hosting services

INTRODUCTION

Typically, the applications used for file transfers and storage are web based and hence require web browsers to upload the files on servers. But the problem arises the time required and the limits of a browser to run properly till the file is transferred. This application will allow the uploading of files without disturbing other processes and at the same time user may be able to work in web browsers without hanging up the uploads. The file size varies according the premium or free users.

The application uses compression as well as encryption algorithms for file security and therefore takes more time to upload a file. The key to encryption can be taken by user or a default key for users can be taken according to the design of
application.various hosting services including cloud are available.

ADVANTAGES OF CLOUD AS SOLUTION

Saves time. Businesses that utilize software programs for their management needs are disadvantaged, because of the time needed to get new programs to operate at functional levels. By turning to cloud computing, you avoid these hassles. You simply need access to a computer with Internet to view the information you need. Less glitch. Applications serviced through cloud computing require fewer versions. Upgrades are needed less frequently and are typically managed by data centers. Often, businesses experience problems with software because they are not designed to be used with similar applications. Departments cannot share data because they use different applications.

Ultra large-scale: The scale of cloud is large. The cloud of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise.

Virtualization: Cloud computing makes user to get service anywhere, through any kind of terminal. You can complete all you want through net service using a notebook PC or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.

High reliability: Cloud uses data multi transcript fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service. Using cloud computing is more reliable than local computer.

Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.
High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.

On demand service: Cloud is a large resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used.

Extremely inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully enjoy the low cost advantage. Various application and advantage of cloud computing are listed below:

1. Cloud computing do not need high quality equipment for user, and it is easy to use.
2. Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus
3. Cloud computing can realize data sharing between different equipments.
4. Cloud provides nearly infinite possibility for users to use internet.

CLOUD COMPUTNG SECURITY ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

A. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users .

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose “availability zones” . On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

E. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium is working to develop consensus on early cloud computing standards and practices.

F. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centres maintained by cloud providers may also be subject to compliance requirements.

SUGGESTED WORK

Typically, the applications used for file transfers and storage is web based and hence requires web browsers to upload the files on servers. But the problem arises the time required and the limits of a browser to run properly till the file is transferred. This application will allow the uploading of files without disturbing other processes and at the same time user may be able to work in web browsers without hanging up the uploads. The file size varies according the premium or free users. The application uses compression as well as encryption algorithms for file security and therefore takes more time to upload a file. The key to encryption can be taken by user or a default key for users can be taken according to the design of application.

An advantage of cloud as solution is that it saves time**.** Businesses that utilize software programs for their management needs are disadvantaged, because of the time needed to get new programs to operate at functional levels. By turning to cloud computing, you avoid these hassles. You simply need access to a computer with Internet to view the information you need.

Another is less glitch as applications serviced through cloud computing require fewer versions. Upgrades are needed. less frequently and are typically managed by data centers. Often, businesses experience problems with software because they are not designed to be used with similar applications. Departments cannot share data because they use different applications.

SECURITY MECHANISMS

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered and sending the in splitted format is most ecured way to transfer the data through the network.

AES ENCRYPTION

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits.

The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. After the implementation of the application, it needs to be hosted so that it is available to the end user. For this purpose various hosting services including cloud are available

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends

on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plain-text using the same encryption key.

AES ALGORITHM

1. **KeyExpansion-** round key keys are derived from the cipher key using Rijndael's key schedule.
2. **Initial Round**

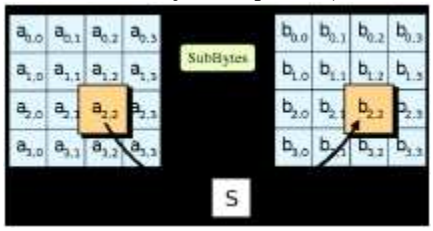
    i. **AddRoundKey:** each byte of the state is combined with the round key using bitwise xor.

3. **Rounds :**

    i. **SubBytes-** A non linear substitution step where each byte replaced with another according to a lookup table.
    ii. **ShiftRows-** a transposition step where each row of the state is shifted cyclically a certain number of steps.
    iii. **Mixcolumns-** a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. **Final Round (**no MixColumns**)**
    i. **SubBytes**
    ii. **ShiftRows**
    iii. **AddRoundKey**

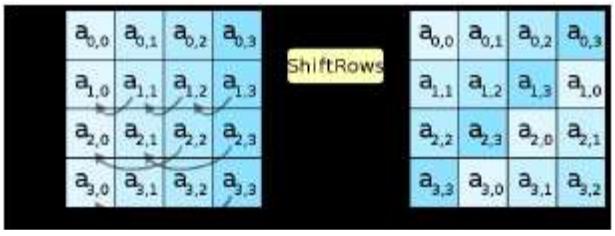
The SubByte step:

In the Sub Bytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF(28), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points



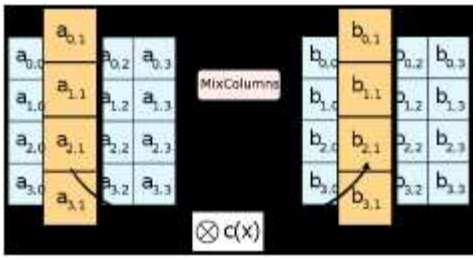
The Shift Rows step:

In the Shift Rows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row. The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For the block of size 128 bits and 192 bits the shifting pattern is the same. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). In the case of the 256-bit block, the first row is unchanged and the shifting for second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.



The Mix Columns step

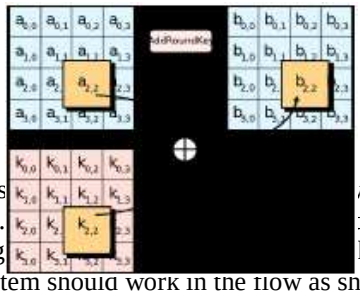
In the MixColumns step, each column of the state is multiplied with a fixed polynomial c(x).In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. During this operation, each column is multiplied by the known matrix that for the 128 bit key.



The multiplication operation is defined as: multiplication by 1 means leaving unchanged, multiplication by 2 means shifting byte to the left and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x11B should be
performed if the shifted value is larger than 0xFF.

The AddRoundKey step

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation ( ). In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.



DESIGN

As application developers which platform components are going to allow us to build all of these features. he core design of the application. The system serves the purpose of file hosting holds data. Multiple clients can logged in to the server and share files. The system should work in the flow as shown below:

User should register on website and download the application and install it. User has to log in through the application and performs operation user wants.

The following fig. no. 1 shows the working of the application with all the inner security as well. When client uploads a file it is first encrypted and compressed and then it is passed through the network. It is decompressed and saved in server in encrypted form. When user tries to download the file the opposite process is followed.

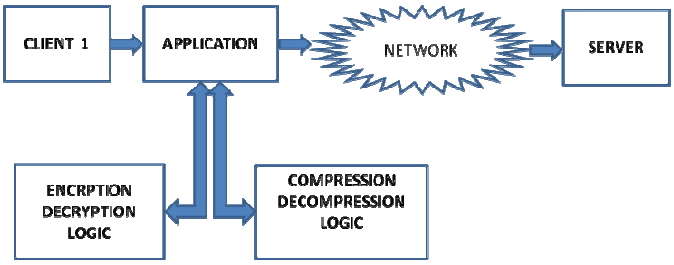


Fig no. 1: System Architecture

Functionality

The application must be able to upload and download file from server without the client knowing the location of files. The application must provide the options to upload multiple files one at a time. The application must provide data after checking proper authentication of the user. The application must also ask for key while encrypting the file of the user and the same while downloading it from the server.

CONCLUSION

In this paper we have proposed a way to host file with security mechanism as well as in a simpler way of it. Cryptography mechanism shows increase in the level of security of files and compression increases the file transfer rate.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, *On Technical Security Issues in Cloud Computing*. IEEE, 2009.

[2] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hip ods/library.html, October 2007, pp. 4-4

[3] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, Cloud Computing Security Issues in Infrastructure as a Service.Research paper volume 2,2012.

[4] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, Four Edition, 2005, pp 189-193

[5] S. Halevi and H. Krawczyk, Public-key cryptography and password protocols Proceedings of the Fifth ACM Conference on Computer and Communications Security, pp. 122-131, 1998, ACM

[6] Open Grid Forum Research Group on Infrastructure Services On- Demand provisioning (ISOD-RG). [Online]. http://www.ogf.org/gf/event_schedule/index.php?event_id=17

[7] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", IEEE International Conference on Services Computing,2009.

[8] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing" .