Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment

[1]Nisha D. Dable, [2]Nitin Mishra

Department of Information Technology,
RGPV University, NRI Institute of Information Science & Technology, Bhopal-India
Email: [1]nishadable@gmail.com, [2]nitin.nriist@gmail.com

Abstract— Cloud computing is a fastest growing technology. It allows business organizations to use or access different applications, store information without access their personal files. While considering the power, stability and the security of cloud one can't ignore different threats to user's data on cloud storage. File access assure in real technique to the file protection due to untrusted cloud servers. In cloud storage system file entrance mechanism is more challenging issue. This system in consequence produces redundant copies of similar files or involves a completely reliable cloud server. Attacks from adversary user are difficult to stop in cloud storage. In proposed system we are implementing the concept of multiple cloud storage along with enhanced security using encryption techniques where rather storing complete file on single cloud system. The system will split the file in different chunks then encrypt it and store on different cloud. The data required for decrypting and rearranging that file will be stored in metadata management server for efficient retrieval of original file.

Keywords—Multi-Cloud computing, AES, SHA-1, Data splitin, Cloud Storage.

I. INTRODUCTION

The boom in cloud computing over the past few years has led to a situation that is common to many innovations and new technologies: many have heard of it, but far fewer actually understand what it is and, more importantly, how it can benefit them. This whitepaper will attempt to clarify these issues by offering a comprehensive definition of cloud computing, and the business benefits it can bring. Security challenges are still amongst the biggest obstacles when considering the adoption of cloud services. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues the cloud paradigm comes with a new set of unique features which open the path towards novel security approaches, techniques and architectures. This paper provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects.

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third-party, on-demand, self-service, pay-per-use and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software.

Usually, make sure that monolithic system track across various PCs means splitting the file into distinct client and server modules. In such schemes, the client module controlled the user interface and the server provided back-end handling, such as record entrance, printing, and so on. 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. This approach simplified development, management, administration, and often improved performance and robustness, since failure in one computer did not necessarily disable the entire system.

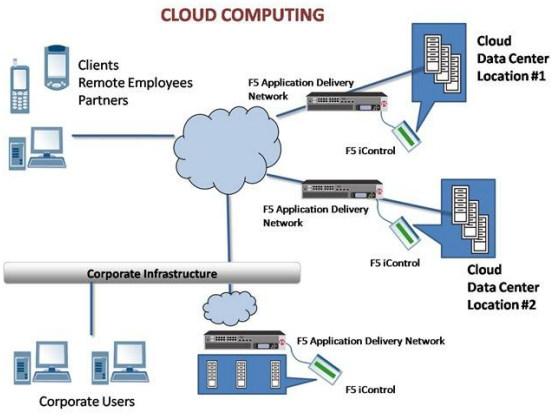

Figure 1 : Architecture of Computing

The ability of the cloud is supported because dividing processes are invoked on behalf of the client. For example, clients can detect a computer (a node) inside the cloud and call a given task; in execution the task, that computer can invoke functionality on other

computers inside the cloud without showing. The further phases or the computer on which they were accepted out, to the client.

With this model, the mechanism of a circulated, cloud-like system can be destroyed down into many distinct packet interactions, or exchanges between distinct nodes. Traditional client-server organisms have two nodes with secure characters and tasks. Modern-distributed organizations can have more than two nodes, and their characters are often dynamic. Once exchange a node can be a client, while in another exchange the node can be the server. In many cases, the final user of the visible functionality is a client with a user sitting at a console, observing the output. In other cases the distributed system functions unattended, performing related operations.

The distributed system may not have enthusiastic users and servers for each specific packet exchange, but it is significant to remember there is a visitor. There is also the receiver of the call (often referred to as the server). It is not necessary to have two-way packet exchanges in the request-reply format of a distributed system; often messages are sent only one way.

II. LITERATURE SURVEY

This approach paper shows that, Cloud Computing becomes thriving and standard business model attribute charming options Additionally to the benefits at hand, the previous options additionally lead to serious cloud specific security problems. The folks whose concern is the Cloud security still hesitate their business to cloud computing. There are main challenges for building a secure and trustworthy cloud system.

The use of multiple distinct cloud simultaneously .The various distinct architecture and introduced discussed according their security and privacy capabilities ans prospects[1]. Cloud computing supply a replacement of computing with varied services models that facilitates completely different services to the users. As all the info of associate degree enterprises processed remotely and exchanges via completely different network. Security is necessary parameter and also the service supplier make sure that there no authorized access to the sensitive information of associate degree enterprise throughout the info information[16]. They security and design a efficient decryption, and also design an efficient attribute revocation method that can achieve both forward backward security[6]. This could be done once, multiple times, or unceasingly. associate degree offender that additionally has access to the process logic of the cloud can even modify the functions and their input and output information. despite the fact that within the majority of cases it's going to be legitimate to assume a cloud supplier to be honest and and accountable manner handling the customers' affairs during a respectful, there still remains a risk of malicious staff of the cloud supplier, palmy attacks and compromisation by third parties, or of actions ordered by a subpoena.

III. REASERCH METHODOLOGY AND IMPLEMETATION METHOD

Development Phases:

Step 1: 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.

Step 2: 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.

Step 3: 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.

Step 4: File encryption technique module

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.

Step 5: 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.

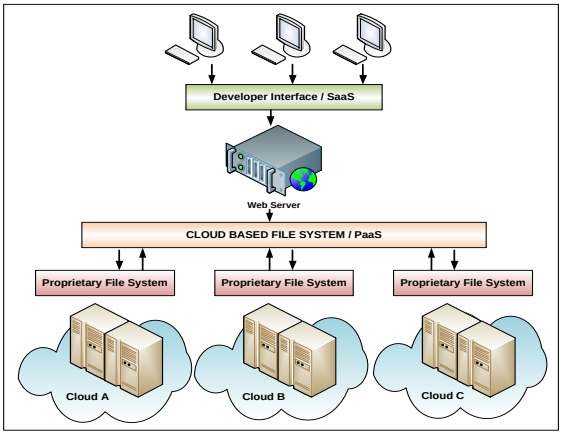

Figure 2 : System Architecture

The basic plan is to use many clouds at constant time to mitigate the risks of malicious knowledge manipulation, disclosure, and method meddling. This design changed targets the confidentiality of knowledge and process logic. It provides a solution to the subsequent question: however will a cloud user avoid absolutely revealing the information or process logic to the cloud provider? the information shouldn't solely be protected whereas within the persistent storage, however particularly once it's processed.

The idea of this design is that the applying logic must be divided into fine-grained components and these components area unit distributed to distinct cloud. In coding technique, the user encrypts the information together with his public key and uploads the cipher texts to the Cloud. The cloud will severally figure on the encrypted knowledge to get AN encrypted result, that solely the user will decode. The user (or a little trusty non-public cloud) manages the keys and performs the coding and coding operations, whereas the huge computation on encrypted knowledge is finished by AN untrusted public cloud.

AES:

AES relies on a style principle referred to as a substitution-permutation network, combination of each substitution and permutation, and is quick in each package and hardware.[8] not like its precursor DES, AES doesn't use a Feistel network. AES may be a variant of Rijndael that contains a fastened block size of 128 bits, and a key size of 128, 192, or 256 bits. against this, the Rijndael specification in and of itself is specific with block and key sizes which will be any multiple of thirty two bits, each with a minimum of 128 and a most of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, though some versions of Rijandel have a bigger block size and have extra columns within the state. Most AES calculations ar wiped out a special finite field.

- Algorithm:

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round

- Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

4. Final Round (no MixColumns)

- SubBytes
- ShiftRows
- AddRoundKey.

- Security:

The design and strength of all key lengths of the AES algorithmic program (i.e., 128, 192 and 256) ar decent to guard classified info up to the key level. high SECRET info would force use of either the 192 or 256 key lengths. The implementation of AES in merchandise meant to guard national security systems and/or info should be reviewed and licensed by National Security Agency before their acquisition and use.

security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first). However, this option is susceptible to certain chosen-plaintext or known-plaintext attacks, and thus, it is designated by NIST to have only 80 bits of security.

The best attack known on keying option 1 requires around 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, and 2^{88} memory (the paper presents other tradeoffs between time and memory). This is not currently practical and NIST considers keying option 1 to be appropriate through 2030. If the attacker seeks to discover any one of many cryptographic keys, there is a memory-efficient attack which will discover one of 2^{28} keys, given a handful of chosen plaintexts per key and around 2^{84} encryption operations.

SHA1

SHA1 stands for "Secure Hashing Algorithm". It is a hashing algorithm designed by the United States National Security Agency and published by NIST. It is the improvement upon the original SHA0 and was first

published in 1995. SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. SHA1 outputs a 160bit digest of any sized file or input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a 512 bit block size and has a maximum message size of 2□4 1 bits.

SHA1 Algorithm

- Padding
  - Pad the message with a single one followed by zeroes until the final block has 448 bits.
  - Append the size of the original message as an unsigned 64 bit integer.
- Initialize the 5 hash blocks (h0,h1,h2,h3,h4) to the specific constants defined in the SHA1 standard.
- Hash (for each 512bit Block)
  - Allocate an 80 word array for the message schedule
    - Set the first 16 words to be the 512bit block split into 16 words.
    - The rest of the words are generated using the following algorithm word[i-3] XOR word[i-8] XOR word[i-14] XOR word[i-16] Then rotated 1 bit to the left.
  - Loop 80 times doing the following
    - Calculate SHAfunction() and the constant K.
    - e=d
    - d=c
    - c=b (rotated left 30)
    - b=a
    - a = a (rotated left 5) + SHAfunction() + e + k + word[i]
  - Add a,b,c,d and e to the hash output.
- Output the concatenation (h0,h1,h2,h3,h4) which is the message digest.

▪ Download:

Get the file name selected by user read 1st part of file(means file a) from user specific directory and get A and also FTP detail from user get from user name and FTP password user in textbox connect B FTP download 2nd part from FTP. Download file function, we get part B and repeat above process we will get C or part C. we combine 2nd (B) and 3rd (C) part we will get X, then combine i.e. 1st part with X.

Finally we have club file in Byte buffer and save this buffer to memory Stream.

▪ Decrypt :

Get the public key i.e. encryption key from textbox and decrypt the memory stream. We save this memory stream to sever disk in temporary function and redirect web client i.e. browser to this Temp file and browser start download file.

IV. CONCLUSION

By implementing the cloud based storage it solve many business secure and safe storage issues. But on the other side many expert state that it is more risky to put the data over single cloud as it increase the adversary user attack possibilities hence by designing the proposed system we are extending the storage cloud security by distributing and encrypting the data. A web portal which let the user manage his data and the managed data should be splitter over the multiple cloud drive as a chunk of file along with encryption. Proposed system will be tested and demonstrate over a local network or on live storage cloud server.

REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, “Security and Privacy Enhancing Multi-Cloud Architectures”, IEEE Transaction on Dependable and Secure Computing, Jan 2013.

[2] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing”, IEEE Communication Survey & Tutorials, Accepted for Publication, March 2012.

[3] Ayesha Malik, Muhammad Mohsin Nazir, “Security Framework for Cloud Computing Environment”, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 3, March 2012.

[4] Mukesh Singhal and Santosh Chandrasekhar, “Collaboration in Multicloud Computing Environments: Framework and Security Issues”, Published by the IEEE Computer Society, 2013.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom’ “Cloud Computing Security: From Single to Multi-Clouds”, International Conference on System Sciences, 2012.

[6] Kan Yang, Ren, Xiaohua Jia, Bo Zhang, and Ruitao Xie, “DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems,” IEEE 2013.

[7] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Tech. Rep., Sept 2011.

[8] Jing-Jang Hwang and Hung-Kai Chuang, ” A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service,” National Science Council of Taiwan Government, IEEE ,2012

[9] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and =8L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," in Proceeding of IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.3

[11] Kan Yang, Xiaohua Jia, " Attributed-based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2012

[12] M. A. AlZain, B. Soh and E. Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing," in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE,2011

[13] Selvakumar G. Jeeva Rathanam M. R. Sumalatha," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012

[14] Akash Kumar Mandal, Mrs. Archana Tiwari, " Performance Evaluation of Cryptographic Algorithms: DES and AES," in Proceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE 2012

[15] J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D," Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm," in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010

[16] Prashant Kumar, Lokesh Kumar," Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 1, December 2013

◈◈◈