ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering | e–ISSN: 2067 – 3809
Tome XIX [2026] | Fascicule 1 [January – March]

[1.] Himanshu MONGA

AN ANALYSIS AND SECURITY MODEL FOR PROTECTED STORAGE FOR CLOUD COMPUTING

[1.] Directorate of Technical Education, Sundar Nagar (Mandi), HP, INDIA

Abstract: Protecting the security of Cloud computing is an important component of the cloud environment and is often stored by the users where the complex information is with the cloud storage providers, but these providers are not trustworthy. That being the case, the written works seek to highlight cloud computing security issues, and found that 50% of cloud computing security issues are related to "single cloud" which led to a decline in popularity among users due to threats of service availability failure and the chance of malicious insiders in the single cloud. In this paper, we propose a new system to improve the security of the delivered cloud storage service via multiple-cloud computing and to develop a novel way for providing a secure data storage system that is easy to install, configure, and use with a compatible multiple-cloud model. This paper focuses on a secure low-cost multi-cloud storage security model in Cloud computing which holds an economical distribution of data across various service providers available in the market for secure storage with data availability.
Keywords: Cloud computing, security, storage, multi-cloud

INTRODUCTION

Cloud computing is a type of on-demand computing service that provides different computing resources over the internet like applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, etc. Users can access and manage their data virtually shared among a pool of servers in real-time. The use of computing resources from anywhere anytime across the globe. It allows users to rent and use a computer system of the desired specification virtually as long as they need rather than spending on a physical one. It enables users to store, manage, and share their data instantaneously.

Even though Cloud Computing is one of the trending technologies in the world of computing, it has its own drawbacks. Security and privacy are the major concern about cloud computing. Because data management and infrastructure management in the cloud are outsourced, transmitting sensitive information to such providers is always risky. Users do not have physical possession of data stored in the cloud.

Recently many cloud storage services have been proposed but most of them focus on the single specific organization, file formats and centralized storage. Additionally, most providers use attribute-based encryption, which encrypts only specific database fields, reducing the reliability of many individuals and organizations. Therefore, cloud security is important to keep the file safe in the cloud. Securing cloud data from anonymous threats is a complex and challenging task. There will be users who will be waiting for the secret keys for a long time, which will reduce the efficiency of the system. Additionally, single cloud storage includes storage limited services, which can be detrimental. In the single cloud storage, data can be easily accessed by malicious insiders.

Many similar approaches have been proposed but failed to implement an effective architecture and working procedure for the secure data sharing using the single-cloud storage providers. The existing approaches does not guarantee the automation of file slicing, encryption, decryption and retrieval process. If an encryption process is done before slicing very large files or video files cannot be uploaded securely and in addition it may also result to wait the user for a longer time.

To address the issues in the existing approaches, we propose a method that ensures confidentiality, secure data storage and file sharing through multi-cloud environment thus by improving the security of the delivered cloud storage service. Multiple cloud computing provides storage services in a single heterogeneous environment. For ensuring more security in multi cloud environment, encryption technique can be used as primary security.

In the proposed framework, data which is uploaded by the user can be sliced into several blocks and encrypted using algorithm then it can store it on the cloud server. Symmetric key or secret key algorithms are the best choice for such applications for storing data in multi-cloud environment. Secret-key encryption algorithms are well suited for performing cryptographic transformations on large streams of data. A key exchange algorithm is

used for file sharing. Our novel approach prevents intruder attacks and authenticates data sharing. The process of Automation includes file uploading, splitting, encryption, decryption, downloading etc.

The rest of the paper is organized as follows. The related work is discussed in Section II, followed by proposed system in section III, result in section IV and conclusion in section V.

RELATED WORKS

In this section, we briefly discuss about the different security challenges and privacy protection mechanisms. In the paper [5], the authors sought to address some of the most common and detrimental security challenges in the cloud. And also discusses the existing security approaches to secure the cloud infrastructure and applications and their drawbacks. Some of the security threats discussed includes Insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, and service disruption. This study is centered on growing a comprehensive cloud-conscious safety approach that could meet the aforesaid studies demanding situations and features cloud infrastructure and ability to protect different layers (including network connections, data at rest, data in transit, applications and VMs) against threats that may arise from within or outside the providers community. The safety approach is meant to leverage the present safety (ad-hoc) technology and using them in a fluid and dynamic cloud environment. In the paper [6], the authors mentioned approximately cloud computing security issues, mechanism, and required situations that cloud provider issuer face all through cloud engineering and provided the metaphoric study of diverse algorithms. The various issues and concerns related with cloud computing are data security, trust, expectations, regulations, and performances issues. One of which is, not so trustworthy management of data: malicious attackers on the cloud and failure of cloud service. For ensuring the security of data on cloud, different algorithms like RSA, DES, AES, Blowfish have been used to compare and study various features among them. DES, AES, Blowfish are symmetric key algorithms. RSA is a public key / Asymmetric key algorithm that uses different keys for encryption and decryption purposes. From the experimental results it is found that AES algorithm uses least time to execute data. Blowfish algorithm has least memory requirement. DES algorithm consumes the least encryption time. RSA consumes longest memory size.

Paper [7] focuses on securing data transfers using encryption techniques. The system also concerned about the third-party auditor issue. Here the author encrypts the data using AES encryption technique since the data is to be send for storage to the cloud server. As AES encryption technique is used for data transfer, this negates the possibility of the system to be unavailable at the time of arrival of big data. Chances of infiltrators trying to disguise themselves as a third party is eliminated since access to the third party is denied. In paper [8], the author discusses a secure file sharing mechanism for the cloud using disintegration protocol (DIP). The author also introduces a new seamless file sharing technology between different clouds without having to share an encryption key. This work uses a combined approach using cryptography and unique network architecture of DIP. This helps to achieve a seamless inter-connectivity between such clouds. Re- encryption functionally of the AS server, allows easy dealings with heavy duty or continuously streaming data upload and download across different geographic locations worldwide. Distributed nature of DSs provides us with greater data independence, enhanced security, all time availability and versatile load balancing.

Lihao Xu propose a new approach to maintain ensure-encoded data in a distributed system using space efficient k-of-n erasure codes where n and k are large and the overhead n−k is small [9]. The authors look onto a system using the protocol to build d an industrial-strength distributed disk array with cheap adapters to connect disks to a network, powerful machines to serve as the array nodes, and highly-efficient erasure codes to tolerate multiple disk and array node crashes. When requests for logical blocks is send by the external parties to the array nodes, array nodes act as “clients” in our protocol, while the cheap adapters act as “storage nodes”.

PROPOSED SYSTEM

The proposed system mainly concentrates on secure data storage and file sharing among users. Since the framework is a hybrid crypto system, a key exchange algorithm is integrated with an encryption algorithm which is used to provide enhanced security for data storage and file sharing. Data is distributed among multiple clouds along with data encryption for attaining security in data storage. The methodology proposes, the uploaded files are sliced into different parts and each part gets encrypted and stored on the multi-cloud. This method ensures that file cannot get access without the permission of the owner. Data owner can upload the files into the proposed framework and splits the file according to the size and the number of cloud storage locations chosen then encrypts each part of the file with a secret or private key provided by the owner. The important thing is that the secret or private key can be further divided based on the number of cloud service providers. Each part of the encrypted file gets stored in the owner’s local machine and then transferred to the multi-cloud servers. Data owner can define the

slicing of the uploaded file. Also, the data owner can share their files into other users through receiver's credentials. The proposed system retrieve the file parts and each parts get decrypted, merged and stored the receiver's machine. The proposed work guarantees that file slicing is based on the number of storage services.

System Procedures

The proposed work is a web application and it has been described with the overall system flow and various procedures. The process performed by the system while uploading or downloading a file are:

- File Uploading: Data owner can uploads the file using the proposed framework. In which the registered users can upload number of files according to their needs. And uploaded files can be shared to other users.
- File Slicing: This is the process of dividing the uploaded file into two or more parts based on the file size. In this process file slicing is based on the number of storage providers available in the multi-cloud server.
- File Encryption: This framework encrypts all the sliced files using Advanced Encryption Standard (AES) algorithm. Although AES has the drawbacks, for long text files it produce a weak cipher and it is time consuming. To overcome the above limitations slicing is used to make it strong cipher and user defined secret key is used.

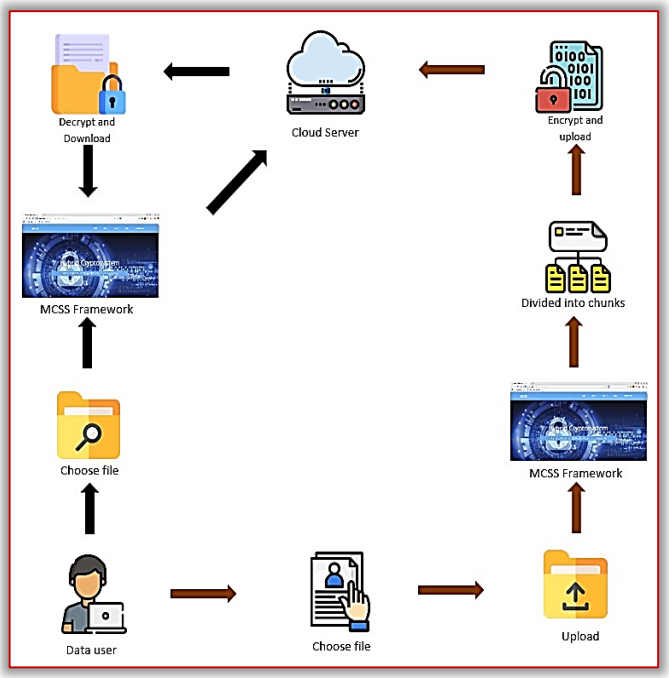

Figure 1: System Architecture

- File Distribution: The process of sending the encrypted files along with user defined key to different cloud storage providers available in the multi cloud server.
- File Retrieval: It is the reverse process of file distribution and file slicing. It is also known as file reconstruction. This framework searches the specified file name in each in multi-cloud server.
- File Decryption: Every file name from the multi-cloud server which is associated with specific file name submitted gets decrypted sequentially and stored in the local receiver's machine.
- File Sharing: In which users can share their uploaded files in the multi cloud location to various users.
- File shuffling: In which users can share their uploaded files are shuffled in the multi cloud location

Algorithm Specifications

- **Algorithm-1: File Splitting and Encryption**

Input: Any text file/image (.doc, .txt, .jpeg, .png, .jpg, .pdf etc.), secret key (SK).
Output: Encrypted Files E(F1), E(F2), E(F3)

- Step 1: Uploads a file(F) and give user defined secret key (SK).
- Step 2: Find the size of a file (SF).
- Step 3: Divide the size of a file based on available cloud providers.
- Step 4: Generate sub keys SK1, SK2, SK3 from the user defined secret key(SK) based on the number of cloud servers.
- Step 5: Encrypt each part of the sliced file with cloud id from local server and store in the multi cloud server.
- Step 6: End

- **Algorithm-2: File Decryption and Merging**

Input: File Name without extension (.doc, .txt, .jpeg etc.), Secret key (SK).
Output: Decrypted File parts and Merged to get file.

- Step 1: Get the file name and secret key from the file owner by making request to the processor.
- Step 2: Enter that file name and secret key.
- Step 3: Perform a search using the associated filename on each multi-cloud storage provider.
- Step 4: Merge each part of the decrypted files from multi cloud storage service provider to obtain the original file.
- Step 5: End

- **Algorithm-3: Key exchange between two parties**

- Step 1: Suppose there are two participants, sender and receiver they generate their own public key (PK) and secret key (SK).
- Step 2: When a sender wants to share a file(F) to receiver, then request to send their public key (PK).
- Step 3: Receiving the public key (PK) from receiver, the sender check authentication.
- Step 4: When authentication is verified, the sender sends an encrypted master key (EK) to receiver.

- Step 5: The encrypted master key is calculated using the secret key (SK) of sharing party with the file upload key.
- Step 6: Receiving the encrypted master key the receiver can download the shared file using their own secret key (SK) with that encrypted key.
- Step 7: End

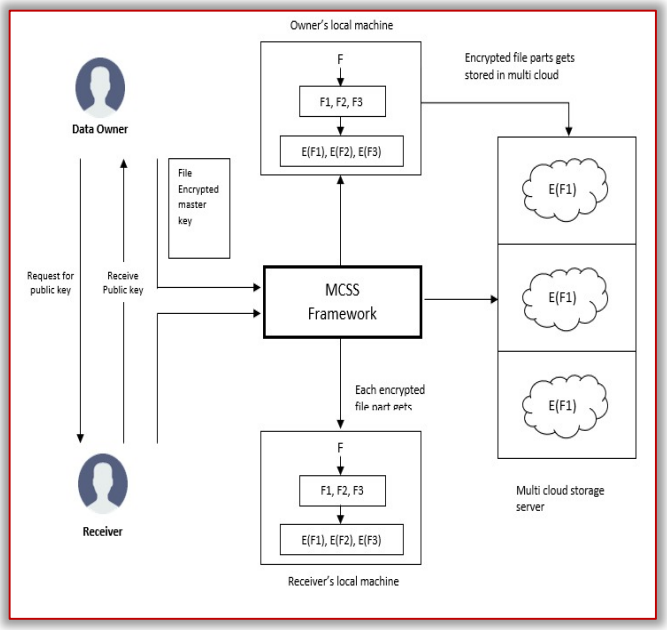

Figure 2: Sharing Architecture

RESULT

The feasibility of the proposed system was studied to identify the potential benefits of developing the proposed system. The study also helped to uncover problems and limitations of the system.

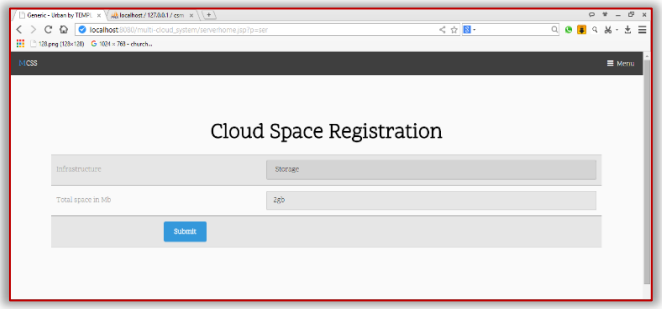

Figure 3: Screenshot of Cloud Space Registration

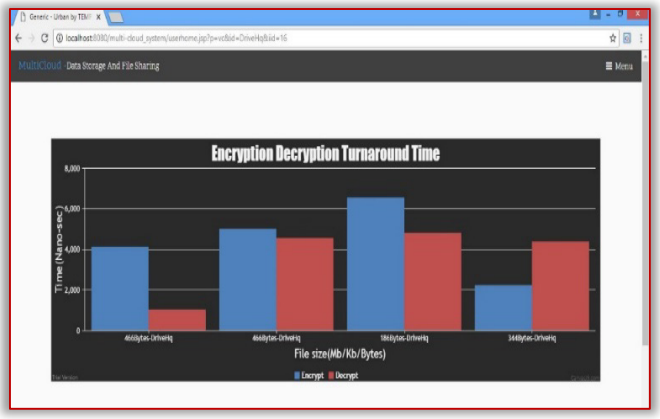

Figure 4: Screenshot of Encryption Decryption Turnaround time

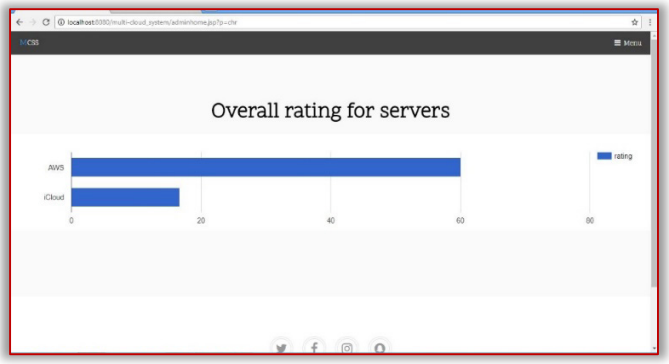

Figure 5: Screenshot of Server rating

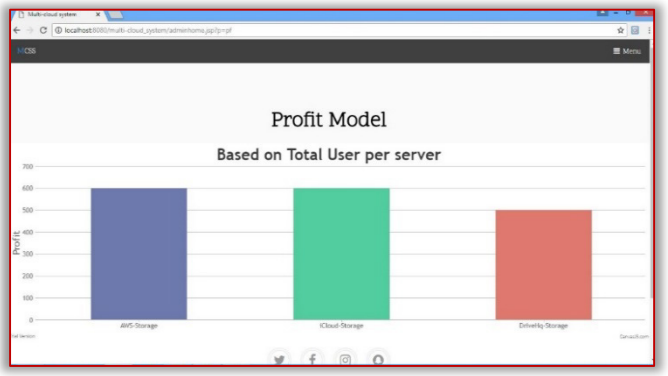

Figure 6: Screenshot of Profit Model

CONCLUSION AND FUTURE WORKS

The proposed methodology is a "Multi Cloud Storage" security framework for both organizational as well as non-organizational aspects. The aim of this work is to provide enhanced security for cloud data storage and authenticated file sharing among various users in the proposed framework. Since various data sets have been used to operate on the proposed model and reached the higher security when compared with other models. The different types of text file formats supported by the system are .txt, .doc, .docx, .pdf etc., and for image formats, it supports .jpg, .jpeg, .png etc., Using Advanced Encryption Standard techniques, these files can be encrypted and decrypted. To enhance the trust of the customers file sharing parts can be defined by using the Diffie Hellman protocol is accomplished in the proposed model. The experimental result justifies the efficiency of the proposed method.

Proposed model ensures the protection of stored data and file sharing among registered users. In which file sharing among only registered users and for public users is done in future directions. Also the encryption of audio files and watermarked data are in the future work. For reducing the users awaiting time we can implement compressed data slicing for encryption.

REFERENCES

[1] Rajdeep Bhanot and Rahul Hans "A Review and Comparative Analysis of Various Encryption Algorithms" International Journal of Security and Its Applications Vol. 9, No. 4 (2015).

[2] Balasaraswathi,V. R., & Manikandan, S. (2014). Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach. In

Advanced Communication, Control and Computing Technologies (ICACCCT), 2014 International Conference on (pp. 1190-1194). IEEE.
[3] Muneer Bani Yassein, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, Yaser Khamayseh, "Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms" ©2017 IEEE.
[4] PengXu, XiaqiLiu, ZhenguoSheng, XuanShan, KaiShuang —SSDS-MC: Slice-based Secure Data Storage in Multi-Cloud Environment 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE) , 2015,pp 304-309.
[5] Akhil Behl — "Emerging Security Challenges in Cloud Computing" 2011 World Congress on Information and Communication Technologies
[6] Rachna Arora, Anshu Parashar – "Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.
[7] Akhil K.M, Praveen Kumar M, Pushpa B.R — "Enhanced Cloud Data Security Using AES Algorithm." 2017 International Conference on Intelligent Computing and Control (I2C2)
[8] Bharat S. Rawal; S. Sree Vivek - "Secure Cloud Storage and File Sharing" 2017 IEEE International Conference on Smart Cloud (Smart Cloud)
[9] M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in International Conference on Dependable Systems and Networks (DSN), 2005, pp. 336–345

ISSN: 2067–3809