### An efficient security framework SINI for securing data in multi cloud storage

Nikita Raychandani1 , Shivani Sharma2 and S. Siva Rama Krishnan3

1 School of IT and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu-632014 [nikitaraichandani33@gmail.com](mailto:nikitaraichandani33@gmail.com)

2 School of IT and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu-632014 [siva.s@vit.ac.in](mailto:siva.s@vit.ac.in)

# Abstract

Cloud computing is new era of the IT industry which bring huge transformation in every paddock. It is used in every big company to store their data. But the challenge faced by customer is which service provider to go with for storing their important data. The aim of our work is to provide a secure multi-cloud service to users with full security to store data between multi cloud storage. So the aftermath will result in secure system of multiple clouds by different cloud providers which can be accessed by multi user geographically with every authentication and authorization only by user.

## Keywords

Cloud computing, multi cloud computing, cloud security, multi cloud security

## Introduction

Now a day’s cloud computing has given industries one level above platform to do any kind of work under one roof using cloud technology. Many organizations are working with the cloud because of its variant feature it provides virtual service which plays a vital role. The high- flying feature obtainable by cloud computing is the cloud data storage, in which; subscribers do not have to store their data on their own servers, where instead their data will be stored on the cloud service provider’s servers. Gradually the computer technology is developing which is helping the environment to the most, now a day’s people are doing all of their work online with the help of technology it involves financial management, transaction, gaming, chatting and many more features which enhance their capability of doing work. In financial transactions it needs more security so as to cover that area cloud gives you security measures to ensure the privacy.

But the major challenge faced by cloud industry is its cost, security and back up all in same infrastructure. As different CSP provides different schemes so the question arises here is what to choose and which is best suitable for the customer.

Different cloud users may have heterogeneous set of requirements based on their work type like if the user deals with the large enterprises then they need large amount of cloud storage

and security of their data and if the user deals with the small companies with less database then they need small amount of the database with security. But in any case the major issue is security and storage.

In this paper, we have elaborated our work by collecting user data and then encrypt data file by dividing into the chunks and finally upload over the cloud system and providing user ability to make smart decisions to choose the best services for them.

Multi user access authentication provided to owner and also power to revoke the access by owner for certain user. Security which involves multi-tier authentication, encryption and generated key for possessor of data and propensity to retrieve back up of data in case of break down condition for one service provider. Distributing the data over different geographical locations for easy access. Henceforth, global access of user’s data from any part of the world over just one click and distribute that data over different clouds.

# Literature Survey

This section states the architecture, cost effectiveness, access control and security mechanism of different schemes. Cloud computing emerges as the best achievement in IT field which has various advantages but good practices always cost something.

The challenge faced by the cloud computing is its cost and security especially from invaders securing the data must be the first priority so Philipp Junghanns et.al. [1] proposes that we can protect our cloud storage by encryption and the reviling the data into your close group with authentication and authorization by using protocols. This protocol involves breaking your data into different parts for secure storage and generates key which is assigned to its users. Cong wang et.al. [2] suggest auditing system for storing data securely with auditing protocol in which one auditor deploy user’s data without passing security measures. Jrad and jitao et.al. [3] proposes that data can be allocated in multidimensional scheme in order to achieve multi- cloud storage. In this data vicinity schedule protocol can minimize the cost related with motion of data and traffic cost bit. Yashaswi Singh et.al.[4] states that to provide user storage at affordable price preventing entrench a service provider in user data. And also it gave best choice to choose their own storage type so if due to any reason one service provider broke down then customer can backup data from other CSP.

The architecture of multi cloud storage is explained in Tsai et. al.[5]in which cloud computing architecture is service oriented which helps in creating, maintaining and reusing the cloud services provided by different CSP. Also this architecture can be achieved by multi-tenancy suggested by XY Li et.al.[6] proposes that the role of CSP is to protect the architecture and user will construct virtual illustration for their own.

The security of this architecture is achieved in proposed work by Bohli et.al[7] distinguish four factors forsecurity of multi cloud architecture includes to collect more than one result from action performed on different clouds ,dividing the system, logic and data into chunk Bellovinet.al[8] proposes that many application uses id and passwords for authentication . And also there are many tools to crack those passwords at freecost so hacker can easily crack passwords proposed by Fanet.al[9].

Zhe Wu et.al.[10] proposes that data storage can distribute over several geographical location to minimise cost also it is more effective then single provider data storage location .In contrast with Bonvin [11] proposes to provide differentiated availability

statistical guarantees to multi cloud storage in case of failure in storing data over geographical locations by applying economical model for cost effectiveness.

Accessing owner data by multiuser can be achieved by private keyword given by a Yanjian yang et.al. [12] in which encryption model used for different user generates query list authorised by owner . And also abrogated user’s loose advantage to search as helper keys get destroyed.

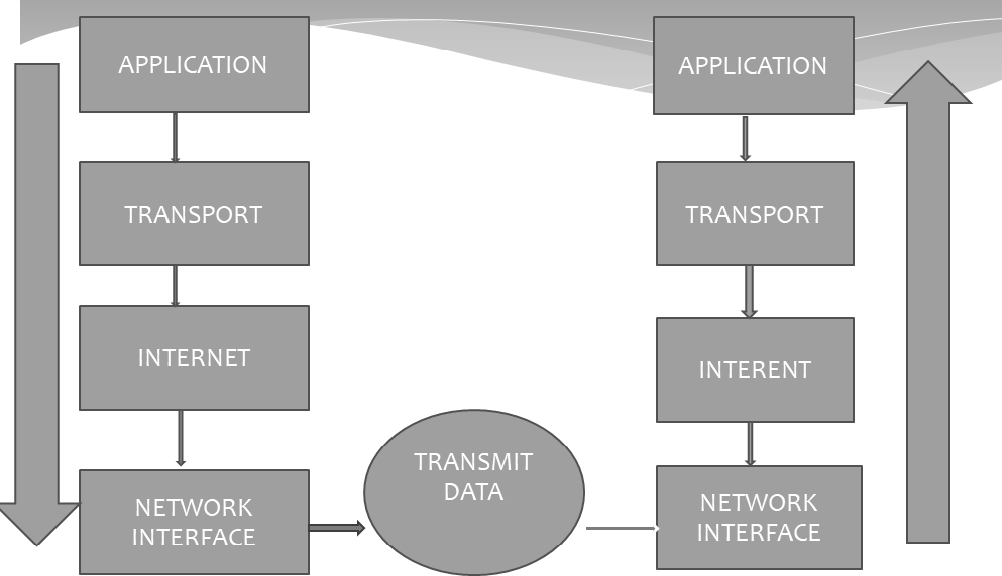
The main challenge with cloud computing is operating and inter cloud realization regarding that Toosi et.al. [13] explore different challenges by proposing classification which recognize facilitator that handle each challenge and converse about future direction. Another challenge in security and privacy Takabi et.al[14] by outsourcing, extend in grand sharing responsibility via SaaS, PaaS, IaaS.

Big data technology can also be a part of cloud computing mentioned by Hashema et.al[15] issued infrastructure to store large amount of data using cloud computing technology. Singh et.al.[16] proposes multi-tier authentication in which there will be 2 level for privacy preservation for improvisation of security. Siva et.al.[17] explains Security framework at each OSI layer that Security at Application layer, Transport Layer and Network Layer.

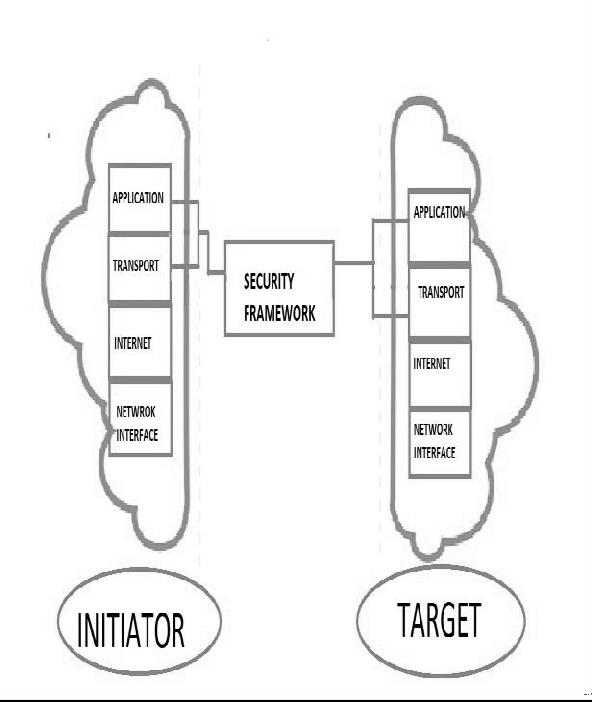
#### Model Description

Siva et.al[18]proposed internet protocol storage which transfer data by encryption. In further addition to that we have added SINI Algorithm for transferring data. The algorithm deals with the encryption and parity checking both on the user side. And when user wants to retrieves the data the same algorithm will do the task of decryption and parity bits removing from the encrypted file.

The following figure represents the process flow of the data in the security model-



Fig(1) Process Flow Diagram



This task will be performed between two components which is initiator process and second is target process. The security framework will work between these two processes. The diagram

description of this task is explained in the following diagram.

Fig(2) functional module diagram

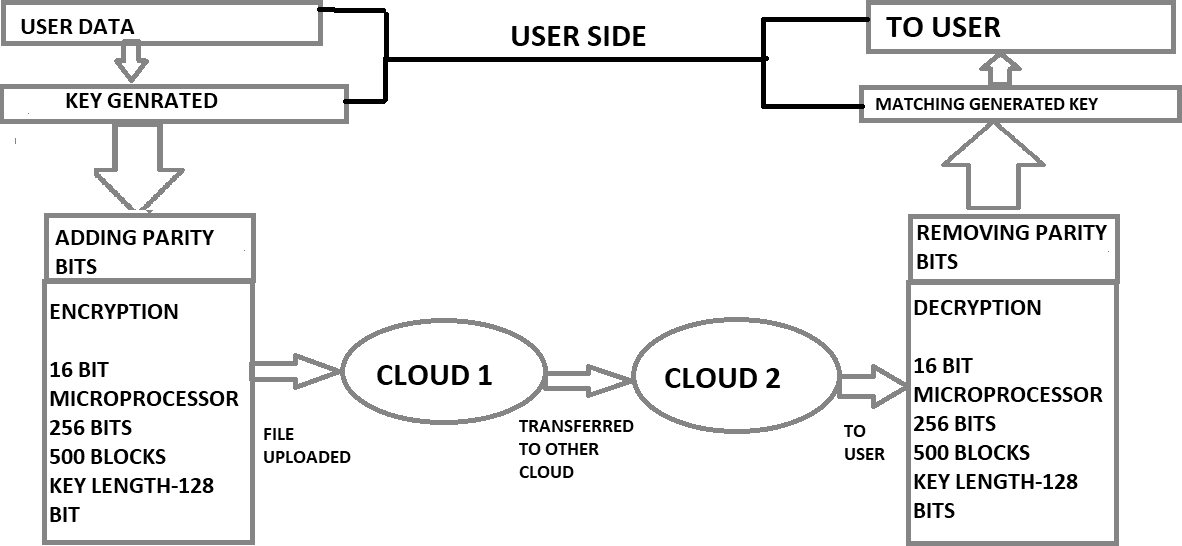
The description of this diagram is divided into 3 main functional modules –

1. Initiator Process- the data given by the user will be accepted in user interface and will be processed by dividing into chunks. These chunks will now get encrypted. Then data will be transmitted to next layer which is transport layer. In this layer parity chunks will be added along with data chunks. Then all these chunks will get transmitted to internet layer in which routing of data will be done. After that data will transport to next layer which is network interface and through that data will be processed to other cloud through security framework.
2. Security framework – encrypted data from the initiated cloud will be transmitted to other different target clouds through VPN. In this we have applied SINI data encryption algorithm which is combination of TWOFISH encryption algorithm

with parity check chunks. This encrypted data now will be transmitted to other cloud and on target cloud decryption process will occur using same algorithm.

1. Target process – in this process the encrypted data will be received by network interface layer which then unpacked at each layer. After that in internet layer will unpack further. Then at Transport layer parity check will be done to ensure DATA INTERGRITY. After further processing data will be transmitted to application layer for decryption.

Henceforth, the architecture diagram we concluded from the above description can be depicted as following.



Fig(3) System Architecture Diagram

**Working of SINI**

The SINI algorithm is the combination of the two fish algorithm and the parity check. Two fish algorithm is basically used of encryption of data. So while dividing the data and transferring from one cloud to another we can use this algorithm along with the parity check to encrypt data and add parity bits with data then transfer it to other clouds services. After collecting the data from user through the API connected with the cloud service that data will be encrypted using SINI algorithm. Then user will enter their password which will act like a key which will be private i.e. only can be accessed by the user. Then data chunks will be uploaded on the multi cloud services.

When user wants to retrieve the data, user has to use the same key which they had used for the password while uploading the data. By doing this they can retrieve their data. The data will be decrypted using same SINI algorithm.

The user can access data at any location globally, as the API from which they can upload or retrieve the data is available online. Also if user wants to share the key with any other trusted person they can do that by generating public key. And also to maintain the security the permission can be revoked from that person by the owner of this service. And regarding the private key will be remain only with the owner.

Hence following is the working of the SINI algorithm after the data received will first changed into the hexadecimal notation then will do the following process-

1. Parity bits

The input data will be converted into hexadecimal notation and the parity bits will be added by using checksum method and then that data will be further processed.

1. Encryption process-

After adding the parity bits’ data will be encrypted using two fish algorithm and then it will generate the private key and then this processed data will be uploading on the multiple clouds.

The following is the pseudo code of the SINI algorithm. Step 1- start

Step 2- read data

Step 3- declare variables a and b (as binary input string) Step 4- hexadecimal sum to find checksum

Step 5- complement the calculated sum Step 6- crypt the data: “data.Twofish ”

Step 7- cipher mode- data.keyLength =256 bit encoding Step 8- stop

While doing the decryption process same steps will be followed in the reverse manner. Hence following figure [19] is the explanation of the encoding and decoding process.

**Key**

CIPHERTEXT

TEXT

**DECRYPTION**

**Key**

TEXT

### Concluding remark and Future scope

**ENCRYPTION**

Hence this security framework is based on the SINI algorithm which works on two fish and parity checker. The data processing stages are processed by first changing data into hexadecimal form then adding of parity bits and then finally the encryption process. The SINI algorithm is significantly used between transferring data between clouds system

confidentiality. Thus, the result of work is to produce secure data which can be transmitted easily within the cloud network.

The future scope of this work is to generate the secure platform for the user to ensure their data is safe on cloud framework. Henceforth this algorithm can provide that ensured to user and it also promotes the cloud computing environment for every firm whether it deals with large or small scale businesses.

#### Abbreviations-

**IaaS:** Infrastructure as a service **PaaS:** Platform as a service **SaaS:** Software as a service **VPN**: Virtual Private Network

### Declarations

*Acknowledgments*

Not applicable.

*Competing interests*

The author declares that he/she has no competing interests.

*Publisher’s Note*

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

#### REFERNCES

* 1. Junghanns, Philipp, Benjamin Fabian, and Tatiana Ermakova. "Engineering of secure multi-cloud storage.
  2. Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." .
  3. Jrad, Foued, et al. "Multi-dimensional Resource Allocation for Data-intensive Large- scale Cloud Applications."
  4. Singh, Yashaswi, Farah Kandah, and Weiyi Zhang. "A secured cost-effective multi- cloud storage in cloud computing."
  5. Tsai, Wei-Tek, Xin Sun, and Janaka Balasooriya. "Service-oriented cloud computing architecture."
  6. Li, Xiao-Yong, et al. "A trusted computing environment model in cloud architecture.
  7. Bohli, Jens-Matthias, et al. "Security and privacyenhancing multicloud architectures.
  8. Bellovin, Steven M., and Michael Merritt. "Encrypted key exchange: Password-based protocols secure against dictionary attacks."
  9. Fan, Chun-I., Pei-Hsiu Ho, and Ruei-Hau Hsu. "Provably secure nested one-time secret mechanisms for fast mutual authentication and key exchange in mobile.
  10. Wu, Zhe, et al. "Spanstore: Cost-effective geo- replicated storage spanning multiple cloud.
  11. Bonvin, Nicolas, Thanasis G. Papaioannou, and Karl Aberer. "A self-organized, fault- tolerant and scalable replication scheme for cloud storage."
  12. Yang, Yanjiang, Haibing Lu, and Jian Weng. "Multiuser private keyword search for cloud computing."
  13. Toosi, Adel Nadjaran, Rodrigo N. Calheiros, and Rajkumar Buyya. "Interconnected cloud computing environments: Challenges, taxonomy, and survey."
  14. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. Hashem, Ibrahim Abaker Targio, et al. "The rise of “big data” on cloud computing.
  15. Sridhar, S., and S. Smys. "A Survey on Cloud Security Issues and Challenges with Possible Measures."
  16. Rakesh, T., Ch Aswani Kumar, and S. Siva Rama Krishnan. "A Proposal for an Optimal Security Model for Cloud."
  17. Somayaji, Siva Rama Krishnan, and Ch AS Murty. "Securing Internet Protocol (IP) Storage: A Case Study."
  18. Hassouna, Mohammed, et al. "An end-to-end secure mail system based on certificateless cryptography in the standard security model."
  19. Muslim, M. A., & Prasetiyo, B. (2016). “IMPLEMENTATION TWOFISH ALGORITHM FOR DATA SECURITY IN A COMMUNICATION NETWORK USING LIBRARY CHILKAT ENCRYPTION ACTIVEX”