ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 7, July 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Refining Data Access Confidentiality in Cloud by Three Server Swapping

Ashwini Raosaheb Taksal[1]
Dept. Of Computer Science and Engineering
Bhivarabai Sawant Institute of Technology & Research
Pune, India

Prof. Sonali A. Patil[2]
Dept. Of Computer Science and Engineering
Bhivarabai Sawant Institute of Technology & Research
Pune, India

Abstract: ***Due to usage of huge infrastructure cloud is blessed with many loop holes of security. Illegal access of the data by the foreign entities is one of them, as one of the main reasons for this illegal access is trace of the data that is going to be stored in one server among the most in the cloud. So Swapping data in between the servers adding more complex pattern than the storing data in straight as this provides more complex job for illegal access entities. Many systems are been proposed to provide the swapping techniques but none of them are achieved much accuracy. As the first step towards this, proposed system put forwards an idea of swapping the data in between the three servers in cloud by dividing the data in 3 chunks and maintaining the controlled roaming of the data over the servers. This process is powered with the data partitioning by maintain server entropy which is catalysed by the Atkinson indices to measure unequal distribution. To increase the level of data security system uses Reverse circle cipher encryption technique with private key concept.***

Keywords: Shannon information gain, Server Entropy, Reverse circle cipher, Atkinson index, Decision Tree.

I. INTRODUCTION

Huge amount of Information is compiled and processed in IT firms on daily basis, demanding huge storage and memory requirement. higher degree of risk is been evolved in maintaining this data .To overcome need of large scale computing time sharing, virtualization with optimized algorithms, better framework, application and infrastructure was taken up in early 70's by scientist and researchers.[7] This prioritization in machines and increased efficiency developed cloud computing terminology. Cloud has powered parallelism in machines and evolved around quality of services (QOS) featuring agility, cost effectiveness, device independence, reliability, scalability and flexibility in implementation. Remote access to required information and lower overhead guarantee an easy access to this bulk information. Cloud provides centralized access and security. With boon of these features in cloud come with security need. Architecture and design of cloud remains huge with complexities and irregularities in infrastructure giving rise to security concerns. Insider attack as well as outsider (hacker) attack. Numerous works have focused on external attack and decisive techniques like "fog computing "in cloud, but higher degree threat remains from inner entities handling cloud centrally. Research work like advanced cryptographic algorithms like SHA512, MD5 along with data compression and shuffling have made though job for intruders and sniffers. Cloud data is been stored on third party servers putting confidential data of users at stake. This data can be accessed by internal user and leads to access confidentially issue, as such cloud system require data access confidentiality ,content coverage confidentiality and even pattern confidentiality .

As three vital methods to achieve most secure system are:

- Pattern Abstraction.
- Content Abstraction.
- Access Abstraction.

Pattern Abstraction: Method to hide Information Access patterns is termed as pattern Abstraction.

Content abstraction: Method to Hide in file been generated is termed as content abstraction.

Access Abstraction: Method to restrict access to very important information to user through layers of access levels.

In Generalized form Security can be implemented at various levels with abstraction.

Contribution of Manuscript:

- ❖ Systematic review of Cloud Computing.
- ❖ Open Challenges and Issues of Cloud
- ❖ Focus on Security Issue.
- ❖ Enhanced Data Swapping Technique for information Security.

A large amount of research is been done on cloud security external and internal both. This manuscript highlights requirement of better security at both inner and external level. Manuscript is been present in six sections section I Introduction II Background III Survey IV core Methodology V Results and evaluation VI conclusion and future Work.

II. BACKGROUND

A. Initial Development of Cloud

Cloud is term which was initially used to refer distributed computing [2] and was initially used to represent components of ARPANET in 1977. Initial development of cloud started at 60's with popularization of virtualization concept and time sharing principle. Future advancement in electronics and telecommunication systems increased bandwidth helps formation of better networks. With need of powerful computing researchers worked on development of software as service ,platform as service and infra-structure as service the pillars of cloud motivation. Cloud computing came to real use in IT firms from 2000 with development of public cloud. Firms like NASA with Open Nebula amazons with elastic cloud largely contributed to expansion of cloud technology.

This is period when it companies started shifting to cloud which greatly reduced cost and increased flexibility. cloud systems are of three types:

1) Public cloud
2) Private cloud
3) Hybrid Cloud

B. Generalized Design of Cloud

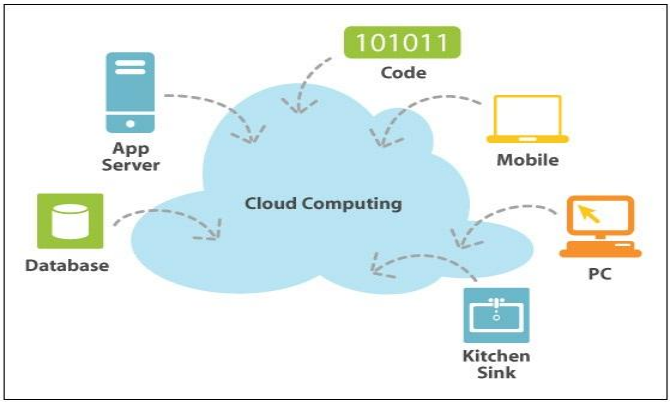

Figure 1: Cloud Computing [6]

Process and flow of information at every phase, device in cloud follows similar step as shown below in Figure [2]

- Process 1: Information generation
- Process 2:Transfer of Information
- Process 3:Usage of Information
- Process 4:Sharing of Information
- Process 5:Storage of Information
- Process 6:Information Archival
- Process 7: Demolition of Information.
- **Procedure 1:** procedure where information is created as core for subsequent operations.
- **Procedure 2:** Procedure to transfer information from node to other
- **Procedure 3: Information usage:** here actually data is been used. Information is present in plain non- encrypted format.
- **Procedure 4: Information storage:** Software as a service or platform as service.
- **Procedure 5**: **Information Archive:** Information consists of user's bank details with userid and passwords which need to be protected. Here set of rules are been enforced for security.
- **Procedure 6: Information Destruction:** unused and unnecessary information for creation and usage needs to be deleted from memory, this procedure guarantee it.

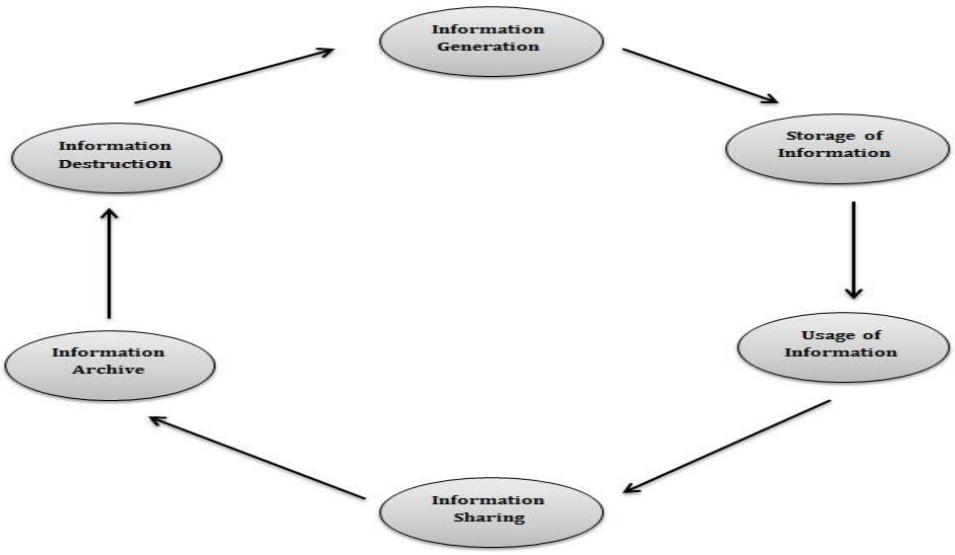

Figure 2: Information Life cycle in Cloud

Basic procedure implemented by cloud service providers for information security is information fragmentation where information is been relocated to different locations or servers for information integrity. Above process creates chunks of information for storage. Numerous algorithms used are broadly classified in accordance to procedure used. Below are procedures listed.

[a] Vertical Fragmentation

[b] Horizontal Fragmentation

[c] Derived Fragmentation

[d] Mixed Fragmentation

Besides above fragmentation techniques swapping of information is better approach for achieving information confidentiality. Swapping technique is decisive approach creating confusion among attackers. Information access pattern get abstracted as information is swapped iteratively.

Any unwanted trying to get access is tracked and receives only bogus or scrambled information.

Swapping techniques are broadly classifieds in two classes:

1. Random swap approach
2. Targeted Swap Approach.

Objective or Targeted swap: This is cost saving technique, based on computation of swap rate in between source to destination variables.

Random swap: swapping operation is been performed for every variable and variable are compared.

Common issue is security when information is been transferred from location to other. With lack of secure mechanism its easy job for attackers to intrude cloud systems.

On of major technique implemented in encryption and widely used for information safety. Cipher string is been generated with encryption algorithm. Pattern of newly generated string is unreadable and completely has different pattern to original information .ABE termed as attribute encryption is most widely used public key encryption technique. Access levels are been used to allow users of different level to have certain degree of access .Attribute based approach is highly preferred as it is one to many approach encrypt-decrypt approach, hence it more secure approach.

Every Encryption algorithm hold key of encryption which decides quality and effectiveness of encryption i.e. if size is more encryption becomes complex and more though to decrypt for attacker. Profile (i.e. name address etc.), time (13:02:34), attribute(i.e. key feature uid.no) are types of key generation mechanism for cryptography process.

Usually attribute encryption can be broadly classified as:

1. Attribute Encryption System with Non-Monotonic Access Configurations.
2. CP-ABE [Cipher text Policy ABE]
3. Hierarchical attribute Encryption.
4. KP-ABE [key policy ABE]

KP encryption String is connected with cluster of features and access procedure has linked top-secret key. Individual who encoded data groups a cluster of expressive attributes mandatory for decoding of information. In state of CP idea of KP is inverted. In this case encryption string is connected with access strategy and individual who encodes Information describes a regular of features mandatory for decoding of Information.

KP-ABE and CP-ABE procedure consists of following steps of procedure in implementation.

1. Arrangement of setup.
2. Generation of Key.
3. Encryption i.e. encoding.
4. Decryption i.e. decoding.

Hierarchical identity based model are as shown in figure 3:

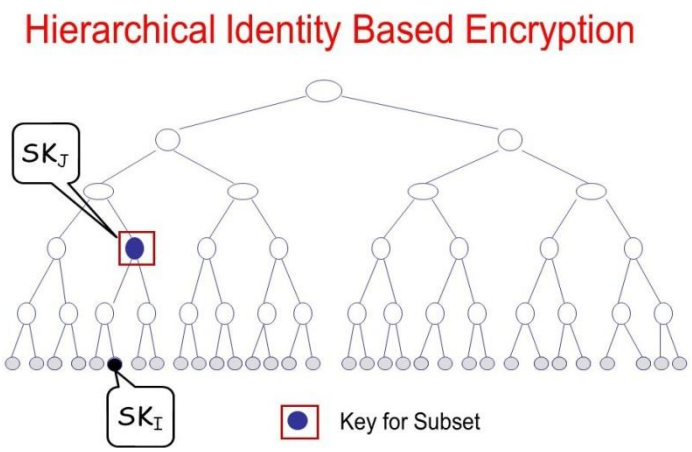

Figure 3: Hierarchical based Encryption [4]

Access controls, efficiency overhead of computation and collusion resistant features have been present in table I which present features and limitations of ABE systems.

Table I: comparative analysis of ABE schemes [3]

Technique /parameter	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Fine Grained Access Control	low	Low, High if re-encryption	Average realization of complex access control	Good	Better
Efficiency	Average	Average, high for broadcast system	Average, not good for enterprise	flexible	scalable
Overhead of computation	High	Most overhead	Average	Some head	Average
Collusion resistant	Average	good	good	good	High collusion

C. Open Issues and Challenges in cloud

Cloud environment and setup is currently under state of infancy it has got open challenges and issues major issues in cloud which are open challenge for researchers are as shown in figure 4.[5] This survey has been done by IDC in 2008 with security having higher degree of issue in all other factors.

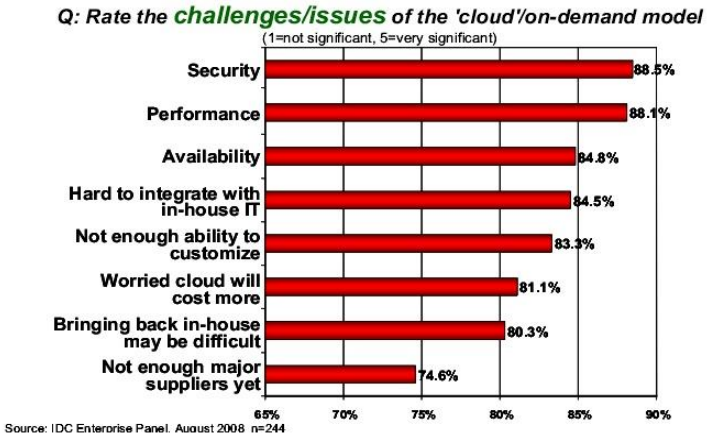

Figure 4: open challenges and issues in cloud [5]

Challenges/Issue=C/I are as summarized following:

C-I 1: security: highest challenge: 88.5%

C-I 2: performance: 84%

C-I 3: Availability: 84%

C-I 4: Integration: 83%

C-I 5: Customization: 81%

C-I 6: Cost and price: 80%

C-I 7: service providers: 74%

As such security is found to be most priority challenge this research work focuses on Security factor of cloud computing future survey and literature work also focuses on security articles only.

III. LITERATURE SURVEY

A. Survey Methodology

Review and detailed survey has been done on articles addressing research issue of security to cloud .ten key from international Journal publications have been reviewed. Pattern of review is core technique, limitations, scope of further work.

B. Survey

In order to guarantee safety of information author [6] presents system for upholding safety and up gradation of information in cloud process life cycle. **Core technique:** Algorithm presented is Diffie-Hellmen, which allows two entities to communicate via common sharing of secret key pass even on unknown channel of communication. Useful in scenario when two entities are completely unknown to each other. **Limitations:** Encryption system is found to have certain open issues. **Scope:** selection of correct Algorithm for Encrypting either asymmetric or symmetric would eliminate bottle lines in security of information.

When user store information on cloud they never trust on singular service provider and opt for information storage by dividing it in small parts of blocks i.e. chunks. Divided blocks are then distributed to select group of service providers (sp). Above process is been controlled through set threshold value, restricting SP being below threshold access value to retrieve information. As such distribution is vital process in Author [7] has presented effective scheme for dividing and dispensing information across multiple cloud .Author has explained dispending schemes like vertical horizontal and mixed approach in deep reviewed for selecting appropriate choice in cloud design easily. **Core technique:** distribution algorithm is been presented for cloud information distribution effectively. **Limitations:** work does not evaluate other distribution algorithms in comparison to proposed work. **Scope:** high amount risk with information been handled by service providers is been reduced, but complexity of procedure can be simplified.

Author [8] Enlarges operative scheme of information dispensing that involves usage of marginal degree of encryption. **Core technique:** scheme is planned in such approach that proficient distribution of information is prepared diagonally in numerous service providers. Shattering is deployed to boards of RDBMS in that each table corresponds to separate entity. This Article author states, proposed scheme upsurges trust of consumers toward SP and also delivers high mark of privacy and security. **Limitation:** proposed system cannot fully abstract information from service providers and there has limitation **Scope:** abstraction of service providers group from each other can add to better approach of confidentiality.

Information dispensing and distribution is been presented in figure 5:

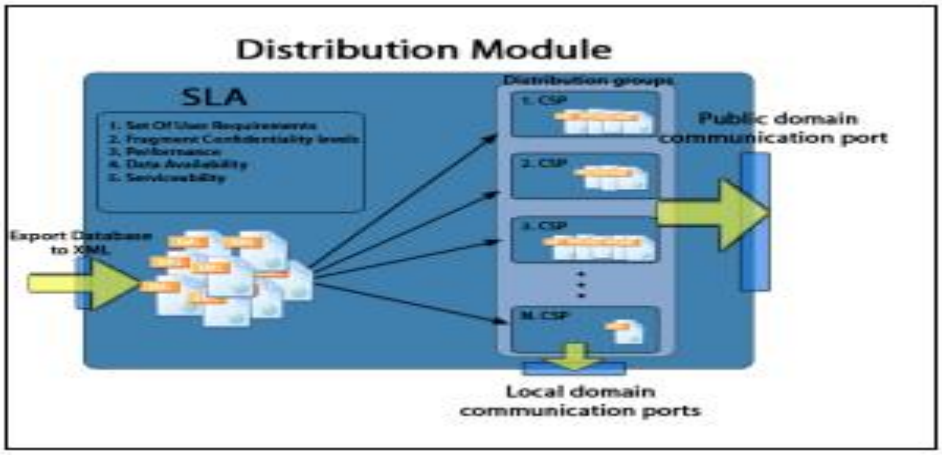

Figure 5: Information Dispensing Model in cloud.[8]

Author [9] explains information swapping, merits of swapping and techniques to achieve information swapping in better way on cloud. Merits and drawbacks of cloud are been highlighted. Role of every entity involved in cloud is been explained like:

- **Service Provider:** Role and Rights.
- **Consumer**/client in cloud.
- **Owner** in cloud

Distinguishing difference among PASS SAAS and IAAS along which flow of information in this layers is been presented. Simple language and pictorial presentation of article help understand cloud terminologies easily. **Core technique:** shuffle index approach is been implemented to maintain abstraction layer on information in case where information is outsourced. Hierarchical encrypted information structure is implemented with index to categorize information in correct way. Periodically location of information is been altered, separating reference of information and physical address. This procedure highly makes tough for hackers or sniffers to attack cloud and thieving target information. **Limitation:** continuous swapping and changing location of information is complex operation hampering system performance as major task process goes in swapping. **Scope:** Integrating periodic swapping procedure with added better technique is required.

Author [10] extends information shuffling work to generate distributed index of shuffling. This distributed index information owner discloses servers for stowage of information increasing information protection in a way and abstraction **.core technique**: distributed shuffle index is been implemented with three layers physical logical and abstraction. Shadow, covers and cache technique deployed in information shuffling is been elaborated.

In cloud Allocating information dynamically numerous flaws rise to eliminate this limitations Author [11] has **core technique:** proposed an effective approach for providing concurrency and compound indexes in outsource information on cloud. This research is extended research on work of author [10].Limitations: comparative examination proves security measured deployed are better as that of [11] but performance analysis is not be computed. Three factors used in empirical evaluation are serial shuffle index, concurrent index where in delta varieties are certainly not resigned, and periodically resigned index. **Limitations:** specifically good for frequency attack only. **Scope**: better protection in for frequency attack scenario as compared to shuffle index.

Mobile cloud is outcome of mobile technology and cloud base technology. Cloud in combination with mobile has uplifted mobile and cellular devices, flexibility of cellular devices is uplifted and assistance to remote operations with cloud and cellular devices.

Author work [12] Engrossed on remote access through cellular devices. **Core Technique:** proposed a method for dividing information streams on cellular cloud. Author say its first of kind system. Proposed work supports dividing information and sharing instance among multiple consumers.

Flexible cloud fabrics have been used as an immoral in development of system offering greater scalability. Framework with genetic procedure is proposed for competent information dividing. Limitation: test results need to best for more parameters.

Scope: genetic algorithm has better results and can be implemented in better way

Figure 6 specify model of information stream dividing.

Every algorithm and approach in encryption is vital as they hold key factor in abstraction and hiding private information on cloud. Cryptographic procedures are classified as:

1. Symmetric

Same key is been used in both encoding and decoding process.

2. Asymmetric

Different keys are used for encoding and decoding information on cloud.

Authors [13] present tabulated survey on two categories of algorithm, just a review work.

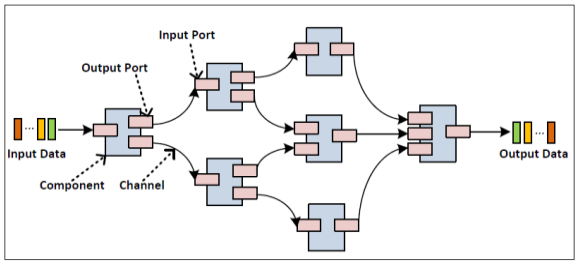

Figure 6: model for information stream dividing in mobile cloud computing.

Table II : symmetric Vs. asymmetric Cryptographic Algorithms.

Procedure/Algorithm	Designed by	Key Magnitude [bits]	Block Magnitude [bits]
AES	Joan Daemon & Vincent Rijmen 1998	256	128
Blowfish	Bruce Schneier 1193	32-448	64
3DES	IBM 1978	112 or 168	64
DES	IBM 1975	56	64

C. Problem Definition

Keeping it simple Problem Definition is: "Design and Development Of security Mechanism in cloud using swapping mechanism. This system must achieve abstraction in information content, access and pattern, through a better encryption system. Simply implementation of information swapping framework.

IV. PROPOSED METHODOLOGY

In core methodology segment research approach in designing framework for information swapping in cloud for confidentiality conserving procedure with under stated steps shown in fig 7 is described.

***Step I*:** Most basic step where all Information of client would be uploaded to cloud storage server, received through cloud controller or web server for further procedure.

Step II: A private key is being produced with random numbers for clients profile information. This key is been used private key for transaction for every user.

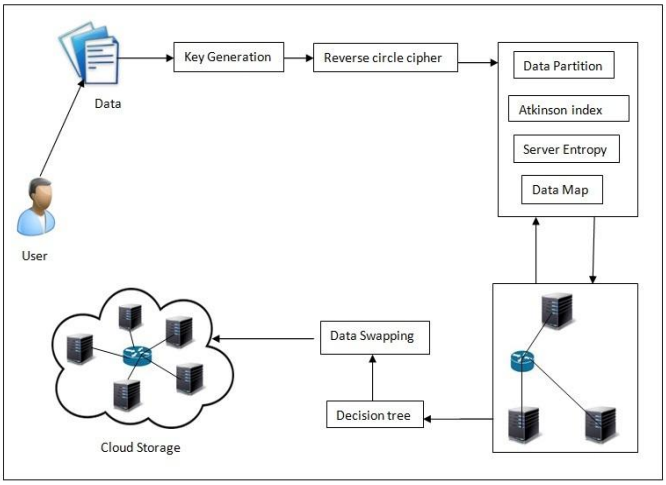

Figure 7: Proposed System Architecture.

PROCEDURE 1: RANDOM KEY FORMATION

Input: Instance Date and time in String
Process:
Step 0: **Start**
Step 1: Get the instance time and date in String Called " $\mathbf{S_s}$ "
Step 2: Remove Special Symbols from $\mathbf{S_s}$ (Like / , -)
Step 3: Get the **MD5** Hash key of $\mathbf{S_s}$ in String as **H1**
Step 4: Assign sum=0 , **Key** =""
Step 5: **for** i=0 to length of $\mathbf{S_s}$
Step 6: sum =sum+ASCII of S_s[i]
Step 7: End **For**
Step 8: Random integer **R1**=sum **MOD** 7
Step 9: **while Key** length is less than 7
Step 10: Select Random character from **H1** on index R
Step 11: and concatenate to key
Step 12: rotate **H1** by one character
Step 13: End **While**
Step 14: return **Key**
Step 15**: Stop**

Output : Private_Key(pk).

Step III: Proposed system implements reverse circle cipher encryption procedure for commanding robust safety policy. RCC (Reverse circle cipher) is safe equated to every other algorithm as it creates and practice use of private key for encryption drive. When input string is acquired it is separated into chunks of 10 letterings. Subsequently these discrete chunks are swapped by their individual index and afterwards give to encryption phase. Encryption section receives swapped string and built on ASCII assessment of every of character encryption is accomplished. Point operation process for RCC procedure is clarified in below section.

Step IV: Information is been divided grounded on numeral of server accessible for swap our system it is set to three, so three lined screens of information is been twisted for operative swap.

Step V: Information swap is initiated from point of unequal information scattering among servers. Above process is been achieved with Atkinson indices operative style of distribution identification as specified in equation I.

Step VI: Sever energy or entropy is not anything but circulation of information amongst all servers, that is been computed by information gain technique using possibility factor as main limitation as termed in equation II.

Step VII: final swap verdict would be booked by examining sequence of assessment stages by decision tree method.

PROCEDURE 2: RRC (REVERSE CIRCLE CIPHER)

Input: File Text **T** and Key **K**

Process:
Step 0: **Start**
Step 1: Create a vector called **DIV** and initialize count=0, initialize String B to empty
Step 2: **FOR** i=0 to length of T
Step 3: Keep joining characters from **T** into String **B**, and count++
Step 4: **If** count =10
Step 5: Add **B** to **DIV**, set count=0 and empty **B**
Step 6: End **FOR**
Step 7: **FOR** i=0 to Size of **DIV**
Step 8: String B_s= DIV[i]
Step 9: rotate B_s by one character, initialize sum =0
Step 10: **FOR** j=0 to length of **K**
Step 11: sum =sum+ASCII of K[j]
Step 12: END **FOR**
Step 13: Val=sum%20
Step 14: **FOR** j=0 to length of B_s
Step 15: ASCII of B_s[j] + Val
Step 16: Replace a new character
Step 17: **End FOR**
Step 18: Concatenate B_s to a string T_E
Step 19: return T_E
Step 19: **End FOR**
Step 20 : **Stop**

Output: Encrypted Text TE

Mathematical Representation

1. CS= {} be as system for Three-server swapping

2. Identify Input as C={D_1, D_2, D_3…..D_n}

   Where C_n= Cloud Data
3. Identify S as Output i.e. Cloud Storage

   S= {C_n, S}
4. Identify Process P
   S= {C_n, S, P}
   P= {K_g, R_c, A_i, S_e, D_c}
   Where K_g = Key Generation
   R_c =Reverse circle cipher
   A_i= Atkinson index
   S_e= Server Entropy
   D_c= Decision tree
5. CS = {C_n, K_g, R_c, A_i, S_e, D_c,, S}

Union of all subset of CS Gives t final proposed scheme.

Equations:

(1)……Atkinson Index calculation can give by

$$A_\varepsilon(y_1,\ldots,y_N) = \begin{cases} 1 - \frac{1}{\mu}\left(\frac{1}{N}\sum_{i=1}^{N} y_i^{1-\varepsilon}\right)^{1/(1-\varepsilon)} & \text{for } 0 \le \epsilon \ne 1 \\ 1 - \frac{1}{\mu}\left(\prod_{i=1}^{N} y_i\right)^{1/N} & \text{for } \varepsilon = 1, \end{cases}$$

Where y_i is individual server load (i = 1, 2, ..., N) and μ is mean load

(2)……$E(s) = \sum_{i=1}^{n} - p_i \log_2 p_i$

V. Results and Discussions

Proposed scheme I designed as web application and tools used for development are java language kit . Private cloud has been developed on three computers . this complete system is tested for authentication . Scheme has been tested for 40 test trails for diverse information upload and swap rates.

MRR is evaluation parameter used to evaluate effectiveness of system and best results are given rank consider first five output . Rank given are 1, ½,1/3….1/5 named as rank reciprocal, whereas MRR is mean value to RR. Equated as with equation3.

(3)……....

$$MRR = \frac{\sum_{i=1}^{N} 1/Rank_i}{N}$$

System has been tested for file of different size and rated rank for from 5 for 10 test trails. MRR calculated is as.

Table III. Consequence of Trial Tests

Sr No	File Size in KB	MRR
1	25	0.875
2	13	0.5
3	15	0.5
4	16	1
5	20	1
	TOTAL =89	MEAN=0.775

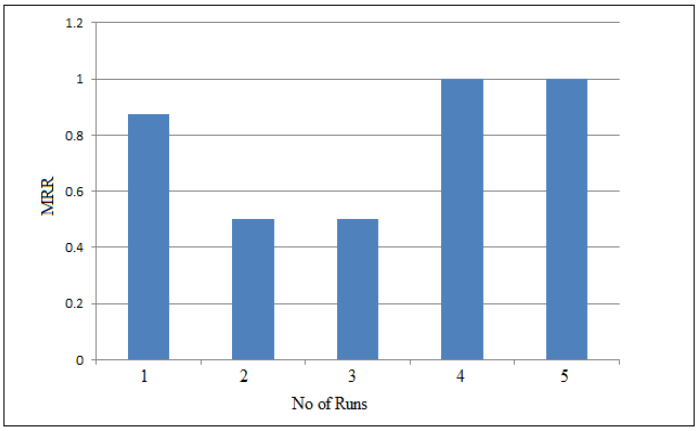

Fig 8:MRR for Different runs

Maximum MRR achieved is 0.755 with different file size and number of iterations.

VI. Conclusion and Future Scope

Proposed Approach absolutely applies information swapping method at three servers or machines used in cloud setup. Formerly swapping information cloud obtains information in encrypted format that is powered with robust encoding techniques like RCC encryption with random key generation procedure

Information in servers is been swapped grounded on inequality of distribution dignified with Atkinson equation and then efficient information swap are accomplished with decision graph.

Proposed Scheme could be advanced to consider more practical parameters for swap operation in cloud like region client type, information sensitivity and addition for effective information swap given N number of server setup at cloud.

Acknowledgement

Author is sincerely grateful to Prof. Sonali Patil, my Project guide and mentor for her valuable guidance and encouragement. Also the authors are thankful to the Computer Engineering Department of JSPM's Bhivarabai Sawant Institute of Technology & RESEARCH FOR their support in providing a good environment and facilities like books, internet and the other resources to complete this research.

References

1. http://computer.howstuffworks.com/cloudcomputing.htm.[online]
2. https://en.wikipedia.org/wiki/Cloud_computing.[online]
3. Minu George ,Dr.c.Suresh Gnanandhas" A survey on Attribute based encryption scheme in cloud computing" International Journal of advanced research in computer and communication engineering vol 2 issue 11nov 2013.
4. http://slideplayer.com/slide/3190808/[online]
5. Tharam Dillon, Chen Wu and Elizabeth Chang "Cloud Computing: Issues and Challenges"2010 24th IEEE International Conference on Advanced Information Networking and Applications1550-445X/10 $26.00 © 2010 IEEEDOI 10.1109/AINA.2010.187
6. Rautela, Sangita, Arvind Negi, and Prashant Chaudhary. "Data Security and Updation of Data Lifecycle in Cloud Computing using Key-Exchange Algorithm."
7. Reddy, B. AmarNadh and P. Raja Sekhar Reddy. "Effective Data Distribution Techniques for Multi-Cloud Storage in Cloud Computing." CSE, Anurag Group of Institutions, Hyderabad, AP, India.
8. Hudic, Aleksandar, et al. "Data confidentiality using fragmentation in cloud computing." Int. J. Communication Networks and Distributed Systems 1.3/4 (2012): 325-329.
9. Barik, Sachida Nanda. "Data Swapping in Cloud Computing." (2015).
10. di Vimercati, Sabrina De Capitani, et al. "Distributed shuffling for preserving access confidentiality." Computer Security–ESORICS 2013. Springer Berlin Heidelberg, 2013. 628-645.
11. di Vimercati, Sabrina De Capitani, et al. "Supporting concurrency and multiple indexes in private access to outsourced data." Journal of Computer Security 21.3 (2013): 425-461.
12. Yang, Lei, et al. "A framework for partitioning and execution of data stream applications in mobile cloud computing." ACM Sigmetrics Performance Evaluation Review 40.4 (2013): 23-32.
13. Mitali, Vijay Kumar, and Arvind Sharma. "A Survey on Various Cryptography Techniques."

AUTHOR(S) PROFILE

Ashwini Taksal, received the B.E. degree in Computer Science and Engineering from Bhivarabai Sawant Institute Of Technology and Research in 2014. Currently she is pursuing her M.E. in Computer Science and Engineering under the guidance of Prof. Sonali A. Patil from Bhivarabai Sawant Institute of Technology and Research from Pune, India.

Prof. Sonali A. Patil, received the B.E. and M .Tech. degree in Computer Science and Engineering and Currently pursuing PHD. She is currently working as an Assistant Professor in JSPM's Bhivarabai Sawant Institute Of Technology and Research, Wagholi, Pune, India.

