IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Migrated Encrypted Data in Cloud using Data Slicing Approach

Rajpreet Kau*r[1], Paramjeet Singh[2], Shaveta Rani [3]

[1] CSE Department, MRSPTU, Bathinda, India
[2] CSE Department, MRSPTU, Bathinda, India
[3] CSE Department, MRSPTU, Bathinda, India

Available online at: www.ijcseonline.org

Accepted: 14/Jul/2018, Published: 31/July/2018

***Abstract*—** Cloud computing is associate coming paradigm that gives tremendous benefits in economical aspects, resembling reduced time to promote, versatile computing capabilities, and limitless computing power. To use the complete potential of cloud computing, knowledge is transferred, processed and hold on by external cloud suppliers. However, data owners are very skeptical to place their data outside their own control sphere. Cloud computing is a new development of grid, parallel, and distributed computing with visualization techniques. It is changing the IT industry in a prominent way. Cloud computing has grown due to its advantages like storage capacity, resources pooling and multi-tenancy. In the proposed system, data to be send to the cloud is encrypted in two steps which are transposition cipher and by encrypting dynamic chunks in lesser time. Proposed system is also evaluated on various parameters like encryption time and data migration time. When compared it is seen that the performance of the proposed system is better than that of existing parameters in terms of evaluating parameters.

***Keywords*—**Cloud Computing, Data Slicing, Data Encryption, Cloud Migration, Cloud Security

I. INTRODUCTION

Various definitions and interpretations of "clouds" and / or "cloud computing" exist Contingent upon the use scope, we will attempt to provides a delegate set of definitions. Distributed computing could also be a model for empowering gift, advantageous, on-request organize access to a typical pool of configurable reckoning assets (e.g., systems, servers, warehousing, applications, and administrations) that may be quickly provisioned and discharged with insignificant administration sweat or specialist organization association.

Other works like [1] outline Cloud Computing as platform or infrastructure within which dynamically climbable (elastic) resources area unit provided as a service through net, enabling users to method the information outside the boundaries of the corporate, providing economical edges through virtualized and shared infrastructure while not the necessity of experience nor information over the underlying technology.

In either definition, each describe a paradigm within which users will demand services through net (servers, applications, infrastructure, development platforms) whenever they have it, sort of a artifact. Take the instance of the recently printed app Cloud Photoshop, a preferred image designer and editor. Customers can use Photoshop and get what they use and wish, no more, no less. This protects the need of shopping for high-priced 1000€ licenses, that represents cost-savings.

A. Cryptography

Cryptography is that the art and science of investigation of outlining or making the mystery message i.e. code or figures of the primary message for the protected correspondence amongst sender and therefore the beneficiary. The principle objectives of cryptography are (1) Authentication, (2) Privacy, (3) Integrity, (4) Non-denial [3] and (5) Access management. Coding is actually a procedure or calculation to form information coated up or mystery. It's thought of because the set of cryptography. It's the real procedure of applying cryptography. It's the procedure to vary or ever-changing over the knowledge into some another frame that offers off a control of being irregular, fatuous and incoherent. It will likewise be aforesaid that coding is that the means toward ever-changing plaintext into the ciphertext wherever plaintext is that the contribution to the coding procedure and ciphertext is that the yield of the coding procedure.

B. Data Slicing

Data slicing is a technique to divide the data into independent chunks. Data can be sliced into three ways which are horizontal data slicing, vertical data slicing and hybrid data slicing. The main idea behind data slicing is to divide the input text into various independent chunks and then encrypt every chunk with a different algorithm to the previous one to provide more security to the encrypted data as it is very

difficult for attacker to decrypt all the algorithms with 100% accuracy and within time.

II. RELATED WORK

K. Gulshan[1], In this paper, intends to address security and protection issues debilitating the distributed computing selection by end clients. Cloud suppliers are aware of cloud security and protection issues and are working barely to address them. Maybe a couple of these dangers have been tended to, yet numerous more dangers still unsolved. In the proposed framework, a secured approach for exchanging the information on cloud is introduced. In the proposed approach input information is divided into three pieces and each lump is scrambled utilizing an alternate calculation and these lumps are then exchanged to the cloud server for capacity. Execution of the proposed framework is assessed and contrasted and existing framework. It is assessed that the proposed framework demonstrates the preferable outcomes over that of existing framework.

K. Ullah[2], Cloud computing rising as a capable vogue to perform large scale and sophisticated method. It expands the information innovation (IT) ability by giving on-request access to pc assets for committed utilize. the information security and protection square measure the vital worries over the cloud from shopper viewpoint. This paper reviews and assesses the planning, information security and protection issues in distributed computing like information secrecy, honorableness, validation, trust, profit level assertions and body issues. The goal of this paper is to survey absolutely these difficulties of information security and protection being looked by distributed computing and basically break down these issues.

R. P. Padhy[3], Cloud process is associate degree engineering for giving reckoning administration by suggests that of the online for the asking and pay per user access to a pool of shared assets specially systems, warehousing, servers, administrations and applications, while not physically getting them. Therefore it spares overseeing expense and time for associations. various businesses, as an example, keeping cash, social welfare and coaching area unit moving towards the cloud thanks to the productivity of administrations gave by the compensation per-utilize style in sight of the assets, as an example, handling influence used, exchanges did, transmission capability exhausted, info changed, or room concerned then forth. Distributed computing could be a whole net subordinate innovation wherever client info is place away and continue within the server farm of a cloud provider like Google, Amazon, Salesforce.som and Microsoft then forth. Restricted management over {the infothe knowledgethe data} might acquire totally different security problems and dangers that incorporate information spillage, unreliable interface, sharing of assets, info accessibility and within assaults. There area unit totally different analysis challenges likewise there for clench distributed computing, as an example, much oversaw profit level understanding (SLA), protection, ability and unwavering quality. This exploration paper diagrams what distributed computing is, the various cloud models and therefore the principle security dangers and problems that area unit as of currently show within the distributed computing business. This test likewise investigates the key analysis and difficulties that presents in distributed computing and offers best practices to specialist organizations and conjointly endeavors desperate to use cloud administration to reinforce their main concern during this extreme financial atmosphere.

III. METHODOLOGY

Encryption is also a way inside that the readable data is processed and born-again into to unclear cipher text. Whole completely different scientific discipline rule applied on segments the rule like AES,DES, 3DES are enforced on individual segments. This individual rule works on each segment at constant time. The plaintext encrypted and born-again into ciphertext. This varied cryptography rule provides a ton of security than mistreatment single cryptography rule to inscribe the data. The technique works in following manner.

A. Data Slicing

Data slicing is finished mistreatment data fragmentation technique horizontal or vertical or mixed fragmentation technique to create the segments of information. The whole data set get into segments either by mistreatment, horizontal data slicing technique. These slices of segments are encrypted mistreatment 3 whole completely different cryptography rule. And then transfer this chunk of segments to the cloud. This chunk of segment use cryptography technique before uploading chunk of information on cloud and once downloading of chunk of information from cloud server. Each chunk encrypted with whole completely different scientific discipline rule.

Data Slicing algorithm steps for the proposed system are given as below:

Step 1: Initially a queue of buckets Q and a set of sliced buckets SB are taken holds only single bucket which contains all tuples and SB is empty. Hence Q= {T}; SB=∅ .

Step 2: For each iteration the systempick out a bucket from Q and separates the bucket in two corresponding buckets. Q=Q-{B}; For l-diversity check (T, Q∪{B1, B2} ∪SB, l); the main condition for the sliced table is that it must satisfies the 1-diversity property.

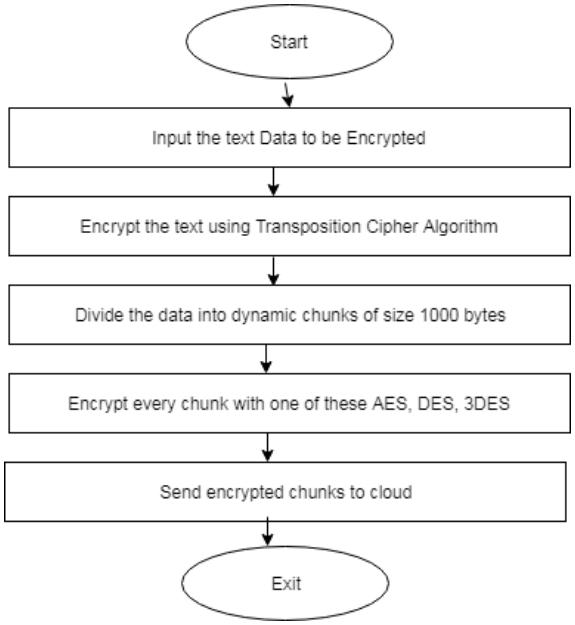
Step 3: For each tuple t of the bucket in the diversity check algorithm, it calculates a list of statistics L[t] having Statistics for therelated bucket B. t∈ T, L[t] =∅. The related

probability p (t, B) and the distribution of key are the sensitive data D (t, B).
Step 4: Q= QU{B1, B2} be the two buckets are then moved to end of the Queue.
Step 5: otherwise SB=SBU{B} for this function it can not separate the bucket further hence it is sent to SB.
Step 6: At the end system return the result SB, and when Queuehas no element in it,system then computes the sliced table. Combination of sliced buckets is SB .So, at last, by the system, SB is returned.

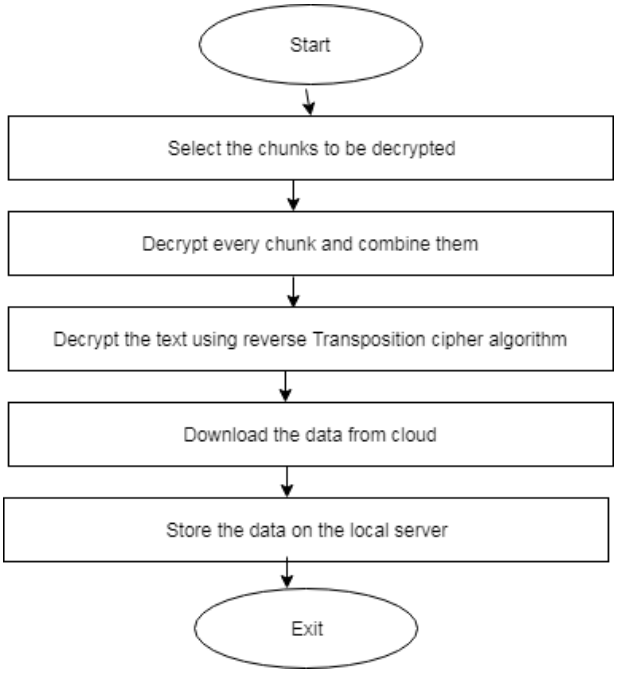
Slicing can handle high-dimensional information and it is the advantage of it. Slicing reduces the spatial property of the data by dividing attributes into columns. Each row of the data provides the output as a sub-table having lower spatial property. Slicing is in addition altogether completely different from the approach of commercialism multiple freelance sub-tables during this these sub tables area unit coupled by the buckets in slicing.

Algorithm steps for the proposed system to encrypt the data are as follows :
Step 1 : Input the text document file to be encrypted.
Step 2 : Encrypt the entire text file using Transposition cipher Algorithm.
Step 3 : Divide the encrypted text into dynamic chunks of size 1000 bytes.
Step 4 : Encrypt every independent chunk with the other encryption algorithms like AES, DES and 3DES.
Step 5 : Send encrypted chunks extracted in step 4 to the cloud.
Step 6 : Exit

Flowchart for the proposed system to encrypt the data are as follows :



Algorithm steps for the proposed system to Decrypt the data are as follows :
Step 1 : Select the chunks to be decrypted.
Step 2 : Decrypt the chunks and recombine them to form a complete text file.
Step 3 : Decrypt the text using reverse Transposition cipher algorithm.
Step 4 : Download the data from cloud.
Step 5 : Exit
Flowchart for the proposed system to Decrypt the data are as follows :



Algorithm steps for the transposition cipher are as follows :
Step 1 : Input the text document.
Step 2 : Extract the characters from the text document.
Step 3 : Extract the ASCII code of every character extracted in the step 2.
Step 4 : Add 1 to the ASCII code of the every character extracted in the step 3.
Step 5 : Convert the ASCII codes of step 4 into their equivalent characters.
Step 6 : Store the output of step 5 as transposition cipher into a temporary variable for further processing.

IV. RESULTS AND DISCUSSION

In this section, we have described the results generated by the proposed system.Proposed system is tested on various input of various types. The proposed algorithm has been implemented using Java Programming language and Cloud Sim as a simulator. The results of the proposed system have

been compared with the existing technique on the basis of encryption time and data migration time.

The proposed system is evaluated using two parameters which are described as below:

Encryption Time: It is time required to encrypt every chunk of data by each of the applied algorithms. This time should be minimum for better performance.

Data Migration Time : It is the time used to migrate the data from local server to the cloud server.

Table : 1.1 The results evaluated by the proposed system are as below:

	DES (in ms)	AES (in ms)	3DES(in ms)	Preprocessing time(in ms)
Data Sample 1	16	15	31	17
Data Sample 2	32	13	15	3
Data Sample 3	16	13	15	21

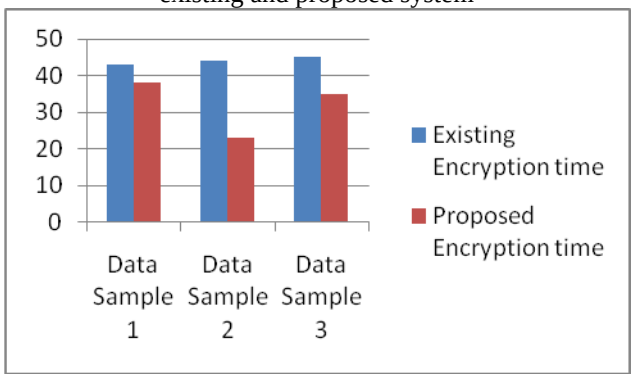
Table 1.2 : Statistics of the proposed system.

Parameter	Value
Algorithms used for encryption	DES,AES and 3 DES
Parameters used	Encryption Time and Data Migration Time

Table 1.3 : Comparison Table for the Encryption time of existing system with that of proposed system.

	Existing (Encryption Time) in ms	Proposed Encryption Time in ms
Data Sample 1	43	38
Data Sample 2	44	23
Data Sample 3	45	35

Figure-1.1 : Comparison graph for Encryption time of existing and proposed system

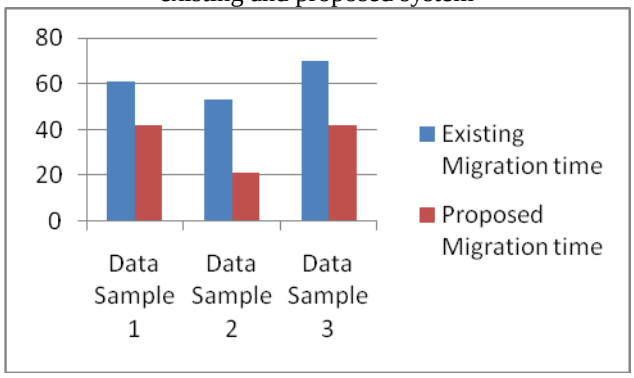


As shown in the above graph proposed system takes less time for data encryption than that of existing system.

Table 1.4 : Comparison table for Data Migration time of existing and proposed system :

	Existing Migration Time in ms	Proposed Migration Time in ms
Data Sample 1	61	42
Data Sample 2	53	21
Data Sample 3	70	42

Figure-1.2 : Comparison graph for Data Migration time of existing and proposed system



As shown in the above graph proposed system takes less time for data migration than that of existing system.

.

V. CONCLUSION AND FUTURE SCOPE

In this proposed scheme, System encrypt the input message in two steps. In the first step whole input text is encrypted using transposition cipher algorithm and output of this step will act as the input to the second step. In the second step, system divides the data into various segments dynamically and encrypt each segment using a different encryption algorithm but with lesser number of rounds to save the encryption time. Performance of the proposed system is calculated on the basis of two parameters which encryption time and data migration time. Performance of the proposed system is also compared with the performance of the existing system and it is evaluated that proposed system gives better results than that of existing system.

In future, Performance of the proposed algorithm can be improved by using hybrid slicing approach and hybrid encryption approach to provide more security to the input data. In hybrid data slicing approach a mixture of horizontal and vertical data slicing techniques can be applied to slice the input data. While in hybrid encryption algorithm a combination of more than one encryption algorithm can be used to encrypt one data slice.

REFERENCES

[1] G. Kumar, V. Laxmi, "*An Approach for Securing Data on Cloud Using Data Slicing and Cryptography*", World wide Journal of Multidisciplinary Research and Development, pp. 371-375, 2017.

[2] K. Ullah and M. N. A. Khan,*"Security and Privacy Issues in Cloud Computing Environment: A Survey Paper*", International Journal of Grid and Distributed Computing Vol.7, No.2, pp. 89-98 ,2014.

[3] R. P. Padhy, M. R. Patra,S. C. Satapathy, "*Cloud Computing: Security Issues and Research Challenges*", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) ,Vol. 1, No. 2, 2011.

[4] S. K. and R. H. Goudar, *"Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey"*, International Journal of Future Computer and Communication, Vol. 1, No. 4,2012.

[5] Hasan Omar Al-Sakran,"*ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT"*,International Journal of Network Security & Its Applications , Vol.7, No.1, 2015

[6] R. Sumithra & Sujni Paul,"*A survey paper on cloud computing security and outsourcing data mining in cloud platform"*,International Journal of Knowledge Management & e-Learning, Vol. 3, No. 1, pp. 43-48 2011.

[7] M. Ahmed and M. A. Hossain, *"CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD"*, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, 2014.

[8] S. Pearson and A. Benameur,*"Privacy, Security and Trust Issues Arising from Cloud Computing"*, 2nd IEEE International Conference on Cloud Computing Technology and Science

[9] S. Y. Koy, K. Jeony, R. Morales,*"The HybrEx Model for Confidentiality and Privacy in Cloud Computing*",2011

[10] A. Goel, S. Goel, *"Security Issues in Cloud Computing"*, International Journal of Application or Innovation in Engineering & Management (IJAIEM),Vol. 1, Issue 4, 2012

[11] C. Patel, S. S. Chauhan, B. Patel, *"A Data Security Framework for Mobile Cloud Computing"*, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2,2015.

[12] S. Y. Hashemi, P. S. Hesarlo, *"Security, Privacy and Trust Challenges in Cloud Computing and Solutions"*,I.J. Computer Network and Information Security, 8, 34-40,2014.

[13] R. K. Kalluri, Dr. C. V. Guru Rao, *"Addressing the Security, Privacy and Trust Challenges of Cloud Computing"*,(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 6094-6097, 2014.

[14] A. A. Soofi, M. I. Khan, *"A Review on Data Security in Cloud Computing"*, International Journal of Computer Applications (0975 – 8887) Volume 94 – No 5,2014

[15] Jayalakshmi S, H. kunder, *"A Review Paper on RASP Data Perturbation for Confidential and Efficient Queries in the Cloud"*, INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING, Vol. 3, Special Issue 1, 2015

[16] Miss. R. Begum,Mr. R.N. Kumar and Mr. V. Kishore,*"Data Confidentiality Scalability and Accountability (DCSA) in Cloud Computing"*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 11, 2012.

[17] L. V. Singh, A. V. Bole, *"Security Issues of Cloud Computing- A Survey"*, IJARCSMS, Volume 3, Issue 1, 2015.

