World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 371-375
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Gulshan Kumar
U.C.C.A, Guru Kashi University, Talwandi Sabo, India

Vijay Laxmi
U.C.C.A, Guru Kashi University, Talwandi Sabo, India

An Approach for Securing Data on Cloud Using Data Slicing and Cryptography

Gulshan Kumar, Vijay Laxmi

Abstract

Cloud computing is an upcoming paradigm that offers tremendous advantages in economic aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. To use the full potential of cloud computing, data is transferred, processed and stored by external cloud providers. 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. On the other hand, the cloud is an open environment and since all the services are offered over the Internet, there is a great deal of uncertainty about security and privacy at various levels. Proposed work aims to address security and privacy issues threatening the cloud computing adoption by end users. Cloud providers are mindful of cloud security and privacy issues and are working hardly to address them. Few of these threats have been addressed, but many more threats still unsolved. In the proposed system, a secured approach for transferring the data on cloud is presented. In the proposed approach input data is fragmented into three chunks and each chunk is encrypted using a different algorithm and these chunks are then transferred to the cloud server for storage. Performance of the proposed system is evaluated and compared with existing system. It is evaluated that the proposed system shows the better results than that of existing system.

Keywords: Cloud Computing, Security, Privacy in Cloud computing, Data Slicing, Data Encryption, DES, AES, 3DES

Introduction

Cloud Computing

Various definitions and interpretations of “clouds” and / or “cloud computing” exist. Depending on the usage scope, we will try to give a representative set of definitions. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Characteristics of Cloud Computing

Multitenancy (shared resources): One of the benefits of Cloud Computing is that it is based on a business model where resources are shared among multiple users at the same time. This is usually reached through virtualization.
Massive scalability: Cloud Computing provides the ability to scale to thousands of systems, and massively scale bandwidth and storage space.
Elasticity: Users can rapidly increase and decrease their computing resources as needed, providing IT resources on demand and address spikes in usage, and release resources when they are not required any more. Elasticity can be achieved by using Load Balancers, which is a mechanism to self-regulating properly the workloads among servers, hard drives, network, and other IT resources.
Pay-as-you-go: Users pay for the resources they use and only for the time they required them.
Self-provisioning of resources: Users self-provision resource like processors, software, storage, network resources... without much intervention from the Cloud Provider.

Correspondence:
Gulshan Kumar
U.C.C.A, Guru Kashi University, Talwandi Sabo, India

Location-Independent Resource Pooling: the resources may be located at multiple places, being this physical separation transparent to the consumer.
Ubiquitous Network Access: Customers can access their demanded services wherever they need them, being either a web browser, several offices on a company, etc

Literature Survey

R.Rogini[1], In the field of computing, cloud computing visualize consistent growth and evolving spontaneously. Still the threats and security problems deal with it. The main focus of this paper is surveying on various privacy preserving concept in cloud computing. This paper is go to handle and examine different steps such as cryptographic step processing, segregation or fragmentation of data, deals with writing access rights and policies. These sort of approaches would preserves the end user data privacy and during public auditing of cloud data privacy preserving is achieved. The inspected approaches are demonstrated and distinguished with one another by stating their merits and demerits. Finally, the concentrated issues to be drawn out in future and centralized results are produced. Earlier outsourcing of encrypted sensitive data, Data access notification to the data owner, providing complete permission of control to user over his/her data. All this function has a capacity to nullify the issues in privacy. In the process of enhancing the privacy preserving approaches in cloud this would serve as a note.
K. Ullah[2], Cloud computing is emerging as a powerful architecture to perform large-scale and complex computing. It extends the information technology (IT) capability by providing on-demand access to computer resources for dedicated use. The information security and privacy are the major concerns over the cloud from user perspective. This paper surveys and evaluates the architecture, data security and privacy issues in cloud computing like data confidentiality, integrity, authentication, trust, service level agreements and regulatory issues. The objective of this paper is to review comprehensively the current challenges of data security and privacy being faced by cloud computing and critically analyze these issues.
Rabi Prasad Padhy[3], Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc.

Proposed Methodology

Data Slicing

Data slicing is done using data fragmentation technique horizontal or vertical or mixed fragmentation technique to creates the segments of data. The whole data set get slice into 3 segments either by using, horizontal data slicing technique. These slices of segments are encrypted using 3 different encryption algorithm. And then upload this chunk of segments to the cloud. On this chunk of segments use encryption & decryption process before uploading chunk of data on cloud and after downloading of chunk of data from cloud server. Each chunk encrypted with different cryptographic algorithm.

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: In every Iteration the algorithm removes a bucket from Q and divides the bucket into two buckets. Q=Q-{B}; For l-diversity check (T, Q∪{B1, B2} ∪SB, l); main requirement of partitioning algorithm is to check condition that sliced table satisfies l-diversity.

Step 3: In the diversity check algorithm for every tuple t, it maintains a list of statistics L[t] contains Statistics about one matching bucket B. t∈ T, L[t] =∅.The matching probability p (t, B) and the distribution of candidate sensitive values D (t, B).

Step 4: Q= Q∪{B1, B2} here two buckets are moved to the end of the Q

Step 5: else SB=SB∪{B} in this step we cannot split the bucket more so the bucket is sent to SB.

Step 6: Thus a final result return SB, here when Q becomes empty we have Computed the sliced table. The set of sliced buckets is SB.So, at last SB is return.
Slicing can handle high-dimensional data and it is the advantage of it. Slicing reduces the dimensionality of the data by dividing attributes into columns. Each row of the data gives the output as a sub-table having lower dimensionality. Slicing is also different from the approach of publishing multiple independent sub-tables in that these sub tables are linked by the buckets in slicing.

Data Encryption

Encryption is a process in which the readable data is processed and converted into to unreadable cipher text. Different cryptographic algorithm applied on segments the algorithm like AES, DES; 3DES are implemented on individual segments. This individual algorithm works on each segment simultaneously. The plaintext encrypted and converted into ciphertext. This various encryption algorithm provide more security than using single encryption algorithm to encrypt the data. The technique works in following manner.

DES (Data Encryption Standard) Algorithm

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is never quoted as such. Every 8th bit of the selected key is discarded, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key. Like other block ciphers, DES by itself is not a secure means of encryption. The algorithm's overall structure is shown in Figure 2.4: there are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). Before the main rounds, the block is divided into two 32-bit halves and processed alternately.

Steps for DES can be described as below:

1. [1] In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.
2. [2] The Initial permutation is performed on plain text.
3. [3] The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).
4. [4] Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key:
    a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.
    b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.
    c. Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step.
    d. Using the S-box substitution produced the 32-bit from 48-bit.
    e. These 32 bits are permuted using P-Box Permutation.
    f. The P-Box output 32 bits are XORed with the LPT 32 bits.
    g. The result of the XORed 32 bits are become the RPT and old RPT become the LPT.This process is called as Swapping.
    h. Now the RPT again given to the next round and performed the 15 more rounds.
5. [5] After the completion of 16 rounds the Final Permutation is performed.
6. The proposed system use 2DES(Double DES) algorithm to perform the encryption on the first chunk of fragmented data.

AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Proposed system use this algorithm to encrypt second chunk of data. Algorithm steps for AES used in the proposed system are given below:

Each round consists of the following four steps:

(i) Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

(ii) Shift Rows: In the encryption, the transformation is called Shift Rows.

(iii) Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

(iv) Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

3DES (Tripple DES)

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. Proposed system use 3DES algorithm to encrypt the third chunk of data. Steps used by proposed system for 3DES are as below:
Triple DES algorithm uses three iterations of common DES cipher.

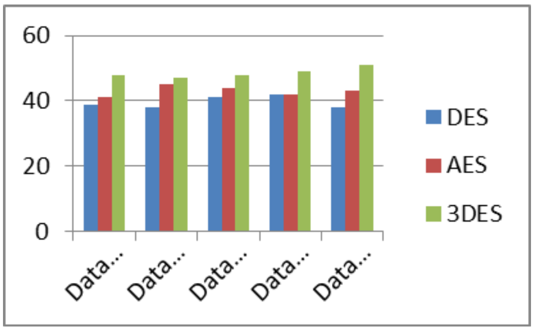
- encryption using the first secret key
- encryption using the second secret key
- encryption using the third secret key

Results and Discussions

This section describes the results generated by the proposed system. We have taken different data sets (Random, Alphanumeric, Numeral, Special characters) and conducted various experiments to determine the performance of the proposed system.
The results evaluated by the proposed system are as below:

	DES (in ms)	AES (in ms)	3 DES (in ms)	Migration time(ms)
Data Sample 1	39	41	48	61
Data Sample 2	38	45	47	53
Data Sample 3	41	44	48	70
Data Sample 4	42	42	49	66
Data Sample 5	38	43	51	59

The above data can be shown in graphical manner as below:



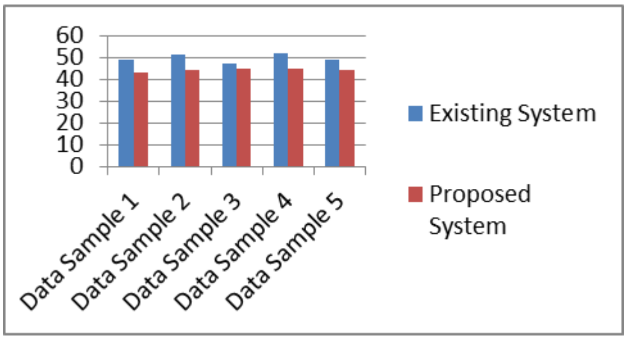
Statistics of the proposed system are as below:

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

Comparison Table for the existing system with that of proposed system is given as below:

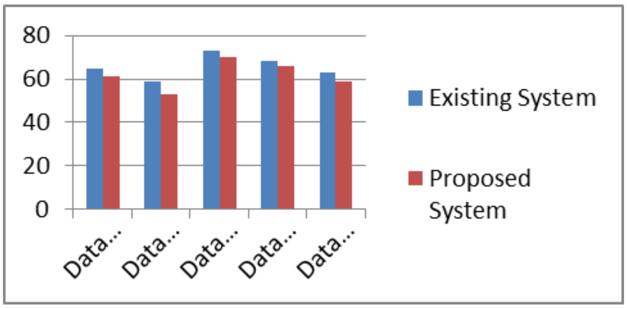
	Existing (Encryption Time) in ms	Proposed Encryption Time in ms	Existing Data Migration Time in ms	Proposed Migration time(ms)
Data Sample 1	49	43	65	61
Data Sample 2	51	44	59	53
Data Sample 3	47	45	73	70
Data Sample 4	52	45	68	66
Data Sample 5	49	44	63	59

The following is the 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.

The following is the 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.

Conclusion and Future Scope

Conclusion

Cloud computing has recently emerged as a paradigm for managing and delivering services over the internet. The rise of this technology is changing rapidly the way of IT, and providing the promise for computation of utilities in a reality. The benefits offered by this technology, the current technologies are not matured enough to realize its full potential. So many challenges are here in this domain Infected Application, Data protection, Availability, Data Verification, Authentication. All this mentioned problems are because of there is not clear method to divide the data into various slices and used different encryption algorithms according to the security of encryption algorithm. In this proposed scheme we divide the input data into three segments and encrypt each segment using a different encryption algorithm. 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.

Future Scope

In future, Performance of the proposed algorithm can be improved by using hybrid slicing approach and hybrid encryption approach. 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. R.Rogini, N.Arun Balaji,"An Inspection On Privacy Preserving Methods In Cloud Computing",International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 5, May 2014,1392
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 (2014), pp.89-98
3. Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satayapathy, " Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
4. Santosh Kumar 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, December 2012
5. Ulrich Greveler, Benjamin Justus, Dennis Loehr,"A Privacy Preserving System for Cloud Computing"
6. Hasan Omar Al-Sakran, "ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT",International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1, January 2015
7. T. Jothi Neela and N. Saravanan,"Privacy Preserving Approaches in Cloud: a Survey", Indian Journal of Science and Technology
8. 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 Volume 3 • Number 1 • January-June 2011 • pp. 43-48
9. Yousef K. Sinjilawi, Mohammad Q. AL-Nabhan and Emad A. Abu-Shanab," Addressing Security and

Privacy Issues in Cloud Computing", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 6, NO. 2, MAY 2014

10. Thota Reshma Kishore, D.Akhila Devi, S.Prathyusha, D.Bhagyasri, Bhuma Naresh,"Client and Data Confidentiality in Cloud Computing Using Fragmentation Method", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013
11. Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing",2nd IEEE International Conference on Cloud Computing Technology and Science
12. Steven Y. Koy, Kyungho Jeony, Ramses Morales,"The HybrEx Model for Confidentiality and Privacy in Cloud Computing",2011
13. Abhishek Goel, Shikha Goel,"Security Issues in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 1, Issue 4, December 2012
14. Chandni Patel, Sameer Singh Chauhan, Bhavesh Patel,"A Data Security Framework for Mobile Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015
15. Seyyed Yasser hashemi,Parisa Sheykhi Hesarlo, "Security, Privacy and Trust Challenges in Cloud Computing and Solutions",I.J. Computer Network and Information Security, 2014, 8, 34-40
16. Rama Krishna 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), 2014, 6094-6097
17. Aized Amin Soofi, M. Irfan Khan,"A Review on Data Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 94 – No 5, May 2014
18. Jayalakshmi S, Harish 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, April 2015
19. Ashima Narang Dr. Vijay Laxmi " Comparison of a New Approach of Balancing the Load in Cloud Environment with the Existing Techniques" published in the INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, in Oct.,2014.
20. Technologies in web intelligence, vol. 6, no. 2, may 2014