Improving Data Security over Cloud at Storage Level Using Efficient Encryption Based Approach

Dushyantkumar B. Sisode
M.Tech IV sem.
Lord Krishna College of Technology, Indore

Vijay Kumar Verma
Asst. Professor (CSE)
Lord Krishna College of Technology ,Indore

Abstract— **Cloud computing is basically a combination of various computing techniques like virtualization, distributed computing, load balancing etc. In cloud computing, there are many data privacy concerns. Data the data over cloud and during communication is important challenge. There are several techniques are used to secure the data at various level in the cloud. To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Network security is becoming more and more important as people spend more and more time connected. In the paper we proposed a efficient encryption based approach for securing data at storage level in cloud environment.**

Index Terms— **Cloud Computing, Data Security, Encryption and Decryption.**

I. Introduction

The cloud computing is a combination of hardware, storage, networks, interfaces, infrastructures, computing power, applications, and services that provide the means through which users can access the, and on demand which are independent of locations. Cloud computing is a way to transfer, storage, and processing of information. The Main advantage of the cloud computing are [12]

1. Reduced IT cost.
2. Business agility support
3. Flexible scaling
4. High availability
5. Les energy consumptions

II. Challenges in Cloud Computing

Cloud computing challenges are divided into two categories.

- Consumer point of view
- Service provider's point of view.

Consumer's challenges are

1. Security and regulations
2. Network latency
3. Supportability
4. Interoperability

Service provider's challenges are

1. Service warranty and service cost
2. Huge number of software to manage
3. No standard cloud access interface

III. Security Issues

Cloud Computing infrastructure is based on new technologies has several major issues such as data security, trust, expectations, regulations, and performances issues. There are three issue are important in cloud computing regarding security.

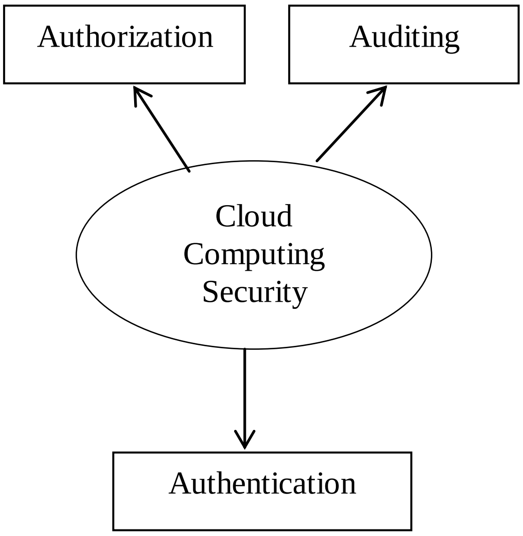


Figure1. Cloud computing security frameworks

Authentication insure that a user is credential are genius; ensure that no illegitimate access is allowed. We can also apply multi factor authentication. Authorization give specific access to a user to resource and define the scope of the access rights of a user on a resource for example read only or write only etc. auditing evaluate the effectiveness of security enforcement mechanism. Securing data at storage level is also important security issue. In cloud environment data is stored

on the servers so it is necessary so store the data in some encrypted form[10,11]

IV. Literature Review

In 2014 Prakash G L ,Dr. Manish Prateek and Dr. Inder Singh proposed "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System". They propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key[1].

In 2013 Ms. Pallavi H. Dixit , Dr. Uttam L. Bombale , Mr. Vinayak B.Patil proposed Comparison of Cryptographic Algorithms on ARM Platform the comparison between two cryptographic algorithm AES and Blowfish algorithm on the basis of ARM implementation[2].

In 2013 Dr. T. Bhaskara Reddy , Miss. Hema Suresh Yaragunti , Mr.T. Sri Harish Reddy, Dr. S. Kiran proposed An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding They considered an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace that pixels into some fixed numbers, generate the key using random generation technique [3,4] .

In 2013 Omer K. Jasim, Safia Abbas, E-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem proposed "Efficiency of Modern Encryption Algorithms in Cloud Computing". They discussed the various encryption algorithms (symmetric, asymmetric) and issues involved in using cloud services such as the performance of encryption algorithms on a cloud environment for different input block data size, how the change in the size of the files after encryption is complete [5,6].

In 2013 Mansoor Ebrahim proposed Symmetric Algorithm Survey: A Comparative Analysis. They proposed comprehensive comparative analysis of different existing cryptographic algorithms (symmetric) based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secure communication (Wired or Wireless[7].

In 2012 Nilesh N. Kumbhar Virendrasingh V. The Comprehensive Approach for Data Security in Cloud Computing: They gives a descriptive knowledge regarding cloud computing privacy and security issue provided by encryption and decryption services. If a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization. This increases the risk factor in terms of security and privacy[8,9].

V. Proposed Algorithms

Data encryption at storage level provides confidentiality and integrity .encryption makes the data indecipherable to unauthorized users. We proposed a simple and efficient method for encryption and decryption data at storage level at cloud.

A. Encryption process

Step 1: Read data character by character.
Step 2: Assign five digit binary codes to each character and form the table.
Step 3: Use an encrypted block is and convert the block into another block of characters of same length and taking column wise value.
Step 4: Store the character block to into Encrypted format and the same procedure for all words.
Step 5: For each word find length and total length of character which is used as key.
Step 6: Stop

B. Decryption process

Steps 1: Decrypt the given key using the block size and taking the value row wise.
Steps 2: Decrypt each character using block size and use row wise character value Steps 1: encrypt the given using the block size and taking the value row wise.
Step 3: Repeat the same value for each word from the encrypted format.
Step 4: As per the given key value and block use the words length from the block
Step 5: Stop

VI. Architecture of Proposed Method

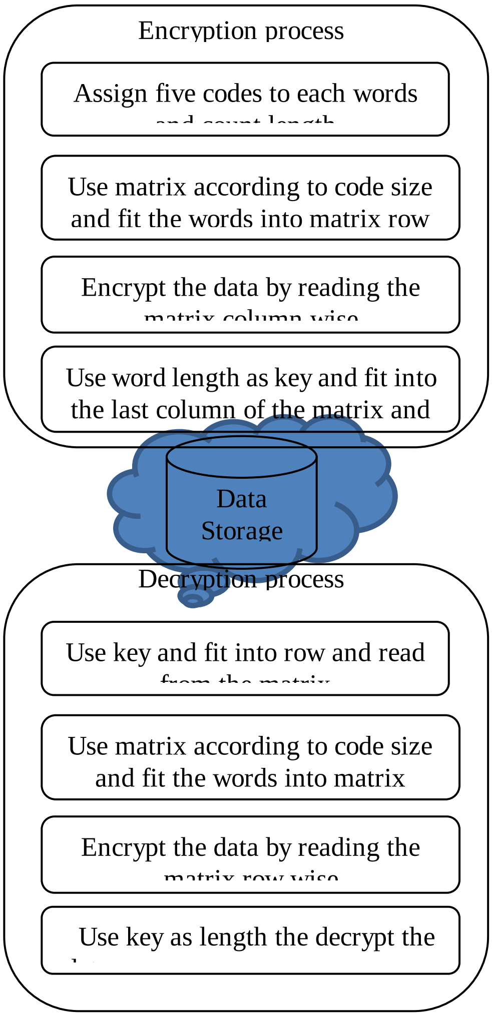
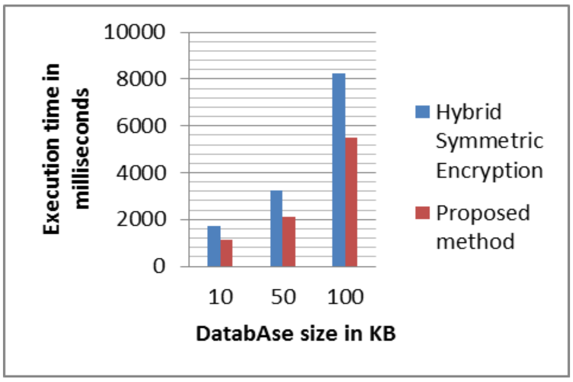

Encryption process
Assign five codes to each words
Use matrix according to code size and fit the words into matrix row
Encrypt the data by reading the
Use word length as key and fit into the last column of the matrix and
Data Storage
Decryption process
Use key and fit into row and read
Use matrix according to code size and fit the words into matrix
Encrypt the data by reading the
Use key as length the decrypt the

Figure2. Architecture of proposed methods

VII. Graph And Analysis

We are using Hybrid encryption techniques and proposed method to compare efficiency. We used different database size and calculate execution time. From the graph it is clear that proposed method take less time to encrypt the data.



VIII. Conclusion and Future Work

In the proposed method we are using five bit code. We are using only alphabets from a to. The proposed code is extendable. As per the number of character increases we extend the code so there is node need to extra bit the code. All the other method used extra bit in the code which is use less con makes the encryption and decryption process difficult and lengthy. In future we can extend this method to include special character also in the encryption decryption process.

REFERENCES

[1] Prakash G L ,Dr. Manish Prateek and Dr. Inder Singh3 Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014 Page No. 5215-5223.

[2] Ms. Pallavi H.Dixit , Dr.Uttam L. Bombale, Mr. Vinayak B.Patil Comparative Implementation of Cryptographic Algorithms on ARM Platform International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2013

[3] An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding Hema Suresh Yaragunti et al, Int. J. Computer Technology & Applications, Vol 4 (6),883-891

[4] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and 4Abdel-Badeeh M. Salem Efficiency of Modern Encryption Algorithms in Cloud Computing International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 6, November – December 2013

[5] Ashwini R. Tonde, Akshay P. Dhande Review Paper On FPGA Based Implementation Of Advanced Encryption Standard (AES) Algorithm International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014

[6] Vineet Sukhraliya, Sumit Chaudhary, Sangeeta Solanki3 Encryption and Decryption Algorithm using ASCII values with substitution array Approach International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[7] Mansoor Ebrahim, Shujaat Khan Symmetric Algorithm Survey: A Comparative Analysis International Journal of Computer Applications Volume 61– No.20, January 2013

[8] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona Analysis And Comparison Of Symmetric Key Cryptographic Algorithms Based On Various File Features International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014

[9] Nilesh N. Kumbhar, Virendrasingh V. The Comprehensive Approach for Data Security in Cloud Computing: A Survey International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012

[10] Suchita Tayde, Asst. Prof. Seema Siledar File Encryption, Decryption Using AES Algorithm in Android Phone Volume 5, Issue 5, May 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[11] Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234

[12] Ms.C.Priya1, Dr.N.Prabakaran2 Security Management in Inter-Cloud Web Site: www.ijettcs.org Volume 1, Issue 3, September – October 2012