International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 720–729

Hierarchical encryption algorithm to secure data fragments in cloud computing

Archana M
Research Scholar
School of Computing and Information Technology,
Reva University, Bengaluru

MallikarjunaShastry P M,
Professor,
School of Computing and Information Technology, Reva University, Bengaluru.

Abstract:

The amount of data getting generated from various resources such as social networking sites, Sensors in IOT devices etc.., which needs to be stored and processed increasing day by day starting from mega bytes to peta bytes and then to zeta bytes. This data can be stored either on server or database but the problem is when it needs to be accessed effectively and also securing this data. Storing real time data and protecting it on server is very tedious task. Today the technology has changed, in order to store data, no need to invest huge amount on physical Infrastructures and also the application software's to store data onto servers. Most of the companies and organizations started using cloud system like MS-AZURE, AWS etc.., to store their data. Cloud Services providers are making task to store and process the data very easy. Initially the data will be divided into number of fragments and then it will be stored in the cloud. But the major concern in this process is security as cloud is maintained by the third part, the trust comes into consideration then how to protect this data it is a biggest challenge. There are so many techniques used by cloud service providers like regular login authentication, RSA, DES algorithms to protect the data. Still the security problem lies with cloud as these are maintained by the third party. The proposed system in this paper will uses the new way of protecting the data, once the data has been divided into fragments. And the encrypted fragment needs to be protected from hackers after storing it on to the cloud. The data needs to be collected back when it is needed and Decryptit to use it further. The algorithm used in this paper is to implement encryption to protect data after defragmentation is secured e-book System with randomization. This method really helps cloud users to protect their data effectively with an efficient system.

Key Words: Code Book, Cloud Computing Defragmentation, Encryption, Fragments.

I. Introduction:

Data is a very important term in Industry Revolution 4.0,as the technology is growingday by day Industrial Automisation has become part of every Industry. As and when technology used in any industry the data is getting generated will be increased and the same data will be used for further process. Consider an example an industry producing blankets, the company cannot succeed in the market if they keep on producing them. There should be huge market survey need to be done and see what is the need of the market and in which locality there is a demand for the product, identify the universal selling point and start selling this product in that particular area. And once they sell the product the company should maintain the data of the existing customers as well as the customers who are interested to buy their product. To maintain this kind of data, before invention of Cloud Computing the companies used to maintain a separate database or Server where the entire data will be stored. Tomorrow when they need this data, the company has to login into the system and search for the data. And whenever the company wants data login into the place where data stored and apply some technical procedures to retrieve and process it when it is needed they need to depend on the third parties. It is a tedious process for Production

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

Company. Again the company has to depend on the person who knows about this technically. What is the solution without affecting their day to day production activities?

Cloud Computing?

Cloud Computing is one of the best way of computing for the companies from one employee to 1 Lakhemployees and so on. The cost to company on physical resources will be reduced and the companies can concentrate on their day to day production, sales and marketing activities. Cloud computing also helps the people understand their business and forecast their future needs and profits etc.., by storing the data of the previous year and this year in cloud to do comparative study to grow further. The data analytics will help top level management to see the entire activities inside the organization to take decision on how to grow further.This is one level of cloud computing where data needs to be accumulated and stored in the cloud.

But the major concern is how to secure this data after the fragmentation process is done before accessed by the customer. That means the organizations need to store their data securely in the cloud, then what are the different methodologies available for effectively protecting the data. Once data is protected and how effectively it is going to be accessed with optimized operations. These are the two major concerns with respect to cloud computing

Cloud Computing is throwing two major issues which needs to addressed with respect to storing the data.

1. Security to the data which needs to be stored on the cloud.
2. Once is it secured and stored, how effectively the data can be accessed when needed that means what are the best practices need to be followed while storing and processing the data.

In this paper the first problem is addressed with respect to securing the data before storing it on to the cloud.

Encryption:

Encryption is the process, which is used to protect the data from hackers or unwanted attacks till it reaches destination or in use. When it comes to cloud computing the data security is major concern as there will be third party who will be maintaining the data and also the cloud data sometimes it is public.

II. Literature Survey:

Archana M, MallikarjunShastry P M "A Method for Text Data Fragmentation to Provide Security in Cloud Computing" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019

This particular paper gave an insight on fragmentation of data in cloud. The data is fragmented based on random number generation. The random number generated and stored it as high and low, based on this high and low values the fragments will be stored. Storing is the first phase in cloud computing, the fragments should be saved in proper order in order to process the data. By considering this paper in the proposed method the data processing is discussed. While storing the data the process of encryption and decryption is carried out.

Aruna T M, Satyanarayana M S, Divyaraj G N "A Unique Work of Out of Sight Epigraphy Creation for Data Security" Journal of Advanced Research in Dynamical and Control Systems Volume 11 No 7 2019.

This particular paper gave an insight on creation of code book and how a code book can help in securing the data. The concept of code book implemented here to encrypt and decrypt the data. The method used in this paper is unique and can be customizable according to the needs of the system. System strength increases based on the customization of the system.

M. Archana P M MallikarjunaShastry "A Review Paper on various Load Balancing Algorithms in Cloud Computing" Vol. 12 Issue 9 2017 P.No. 8579-8585.

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

This particular paper gave pure insight on how load balancing can be carried out in cloud computing in order to optimize data storing and secure system.

MallikarjunaShastry .P.M Abhishek Gaur "Enhanced Approach for Secure Stored Data in Cloud" Test Engineering and Management Volume 83 May 2020.

From this paper gave insight on the how best the security of the data can be enhanced in the cloud computing. The methods in this paper helped in deciding new techniques to implement new security algorithm for data storage in cloud.

III. Proposed System:

In proposed system the algorithm which is proposed is based on one of the ancient methodology called code book system which suits for cloud computing in providing security for data. The ancient methodology has been implemented using new technology like data base and also randomization function and named it as customized encryption book.[2]

Cloud Encryption Book:

As name indicated there will be a book which will be having all the data related to a particular element which stored in fragments[1] and will be saved according to the randomization algorithm as mentioned paper 1 of the reference. This Cloud Encryption Book is going to be random in nature and can be customizable as per the needs of the customer which will improves much more security by protecting the system from hackers.

The concept of Randomization[4], in order to provide security for this book the concept of randomization is used where the entire code book is going to be randomly changed based on the time slice and the time slices will play vital role in this. So that by that time the hacker's reaches to find out the actual message the encryption term will be changed.

IV. Illustration:

How this system will work with respect to cloud computing will be depicted in the below diagram. The data input will be either the data which is entered by the user or the real-time data.

The major consideration for input here is text data of different languages like English and also regional languages as well.

When system is implemented in real time the major concern is on size of the data, that means the user or administrator is not going to have any control on how much data will be processed at a time. It might be kilo bytes or mega bytes or peta bytes etc.., in this proposed method the system is designed such a way that it will be ready to adopt for the scalability problems of data inputs[3]. And also the system is capable of processing data with efficiency and good throughput. This system is tested for different conditions of input before finalizing efficiency of the system.

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

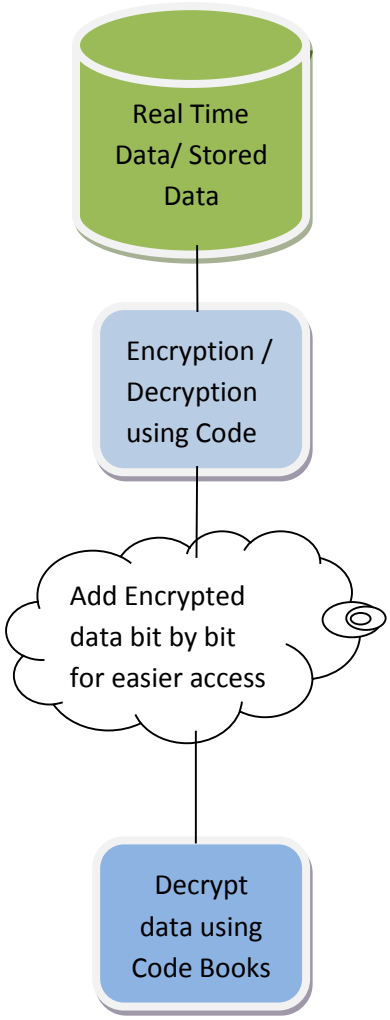


Fig.1. Implementation Procedure

F1	F 2	F 3	F 4	F 5	F6	F 7	F8	F9	F 10

Fig.2. Data Fragment

As shown in above Fig.1. &Fig.2.the F1, F2, F3 and so on represents the data fragments[1]. Once the data fragments have been generated the each and every fragment data will be encrypted using the methodology as proposed in this paper. The entire data will be encrypted according to cloud encryption book. And for each and every activity the cloud encryption book can be created separately so that there won't be any duplication.[5]

V. Cloud Encryption Book Sample Format:

Cloud Encryption Book is nothing but as name indicates there will be a Letter and corresponding symbol which will be stored in the database whenever the data fragments are created corresponding data in data fragments will be compared with this book and will be encrypted accordingly. The entire cloud encryption book will be generated with special symbols, which will increases the complexity of the data for hacker to hack it.

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

S.No	Letter/Number	Symbol
1.	A	↓
2.	a	€
3.	B	¥
4.	b	α
5.	1	҂
6.	2	Ч
8.	3	Ь
9.	,	ϒ
10.	.	✓

Table (1). Sample Code Book

The above sample data code book Table(1) will be used whenever there is a data encryption and thisbook is stored in the cloud based system which is not even known to the cloud owner. The question arises here is if the hacker come to know about this code book he can easily hack the data. To avoid this situation the complexity of code book will be customized based on the application it is going to be used. On top of it the code book will also have random function which will interchange the left side values based on time slice as per the need of the customer in order to increase the complexity. [6].

The problem here is if the cloud encryption book is changing the data which is going to be decrypted will be different compared to the encrypted as the symbols have been changed after some time slice, to overcome this kind of scenario the time stamp of each and every encrypted format and also code book will be saved as archived. Based on the time stamp which code book needs to be used for that particular content will be decided and data will be decrypted which will improves the performance of the system there by enhancing the security of the system. [7] **VI. Cloud EncryptionAlgorithm:**

1. Start
2. Select the data need to be Fragmented
3. Divide the data into fragments
4. Collect the data of each and every fragment
5. Compare the data of each fragment with cloud encryption book
6. Apply encryption process to encrypt the data
   I. Read the characters of the every fragment
   II. Load the character into temporary address location
   III. Search for Same character in the cloud encryption book
   IV. If character matches
      a. Read corresponding symbol
      b. Replace the character with this symbol into the fragment
   V. else
      a. Print the corresponding character not found
7. Repeat step 4 to 6 till the completion of all fragments.

By applying the above algorithm the entire data in the fragments will be encrypted. The major problem here is the time taken for encrypting each and every fragment data it takes some additional time.

To overcome this problem
1. Based on the need or level of security either the number of characters in a fragment will be encrypted.

2. The entire fragment will be assigned with one symbol and it will be stored in the cloud. [8]

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

As discussed earlier in this method the security purely depends on the system or applications which need to be build. And level of security also purely depends on the customer who is going to use it.[15]

The next algorithmin this research work is randomization algorithm as specified in the implementation steps.

The problem occurs when hacker is trying to hack the Cloud Encryption Book directly, the feasible solution here is always modifythe cloud encryption book after particular specified time. In this method the randomization Cloud Encryption Book algorithm is mainly used to modify the symbol by keeping the content fixed. As per the book the symbol has to be changed randomly but the content will be fixed. [9]

VII. Cloud Encryption Book Randomization Algorithm:

1. Start

2. Read the symbol Column in the cloud encryption book.

3. Apply randomization on the symbols.

   a. Read the symbols one by one and store it into array
   b. Find the starting index and maximum length of the symbols store.
   c. Calculate the random value

      Random = CI+4

   d. Check till the Random ==Maximum Length.

Replacethe position of the every symbol.

4. Repeat the loop until all the symbols get interchanges.

5. If condition 3 fails make

Maximum = Maximum Length.

6. Repeat the process again considering the starting value as initial index and maximum value

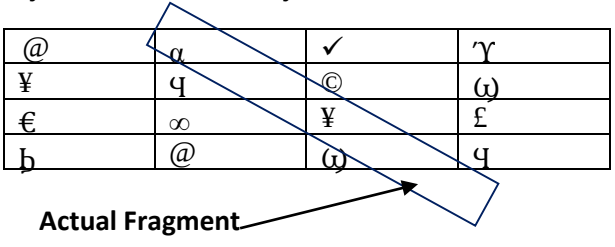
This random function will help to provide multilevel security to the cloud. The Code Book and Randomization will provide maximum security to the data stored in cloud both from the Hackers and also the Public Users.[10]

Once the data get encrypted in order to increase the security the data will be stored in table format, where along with dummy data there will be many dummy variables which will be stored when hacker tried encrypting the data , the hacker does not know which is original data and which is the dummy data. This will kill the time of the hacker which will help in implementing the much more effective Fig.3. Actual Fragment in a Table

As shown in Fig.3. The actual fragment will be stored in a table. The size of the table is directly proportional to the size of the fragment.

Table Size ➔Size of the Fragment*2

system for data security [1]



ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

The means if the fragment size is 4 the table size is going to be 4*2 = 8. It is going to be 8*8 Matrix. This will increase the complexity for the hackers to hack the data.

Here the drawback is if the size of the fragments are getting increased then the table size will increase means there is no limitation on size, how to control the size of the table. [11]

In order to control the table size the concept of data visualization techniques which will helps in data optimization process.

Once the data visualization will be implemented, the customization patterns will be considered to increase much more security for the data which is getting stored in the cloud. The cloud data will be secured at every level, both from hackers and third party.[12]

So overall this system will help the users to store data on the cloud and off the cloud. And as it is automatic process the system does not require any third party intervention in storing the data. The only place the system needs manual intervention is auditing the data which can also be verified multiple number of times in order to reduce data redundancy.[13] **VIII .Results**:

As discussed above initially the cloud encryption book will be created at backend and based on the cloud encryption book the data will be encrypted step by step and same will be stored in table. Here the data will be displayed in the table format.

In this system the encryption will be done for both English and Kannada.

In the first step the data will be read from the user or automatic system and it is encrypted. And same cloud encryption book will be used for the decryption. The system is tested for different sample data and result found satisfactory. And same system has been given to the ethical hackers to check the strength of the system. The ethical hackers tried for a period of 7 to 10 days to decrypt the encrypted text and found it is difficult to decrypt the text. Hence the system found strengthen can be utilized in our ongoing research on cloud security. [14]

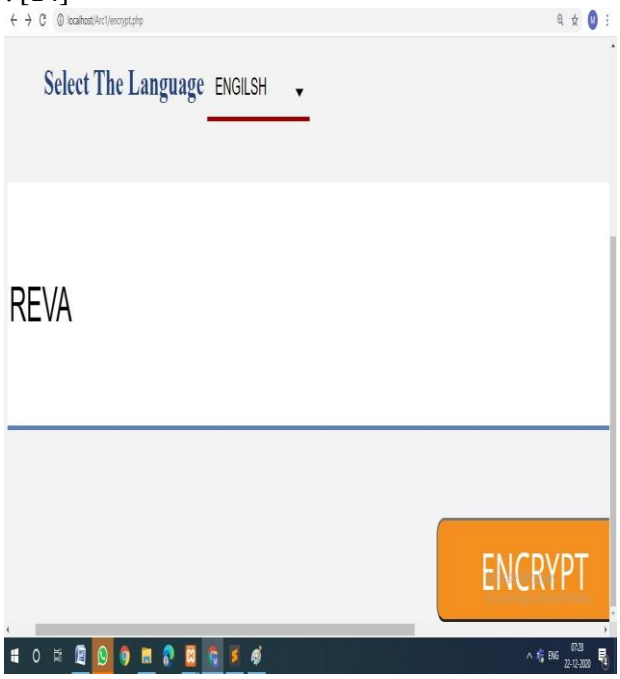


Fig.3. Encryption

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

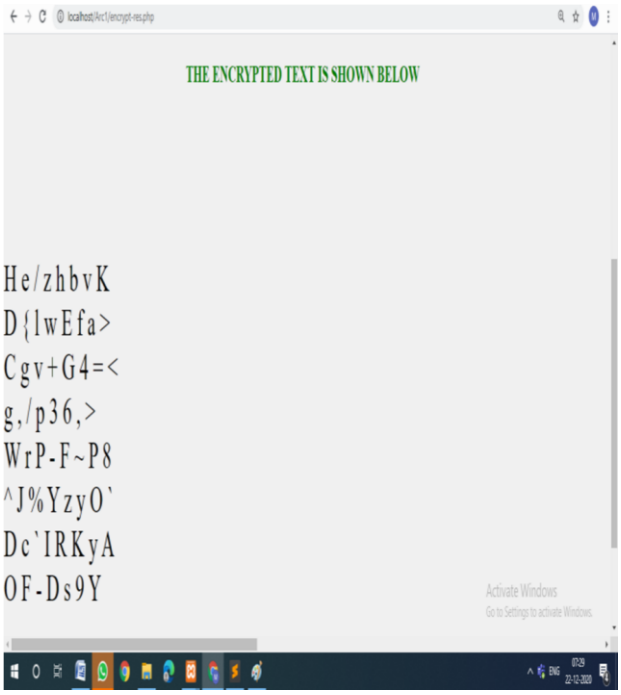


Fig.4. Encrypted Data

Fig.5. Regional Language Entry

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

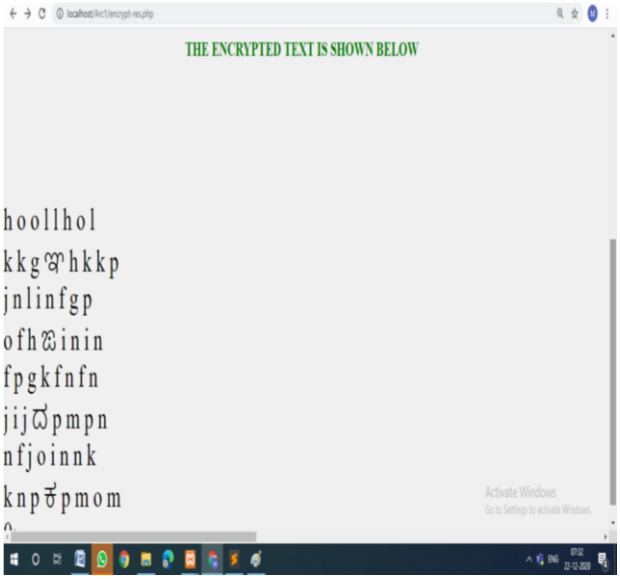


Fig.5. Regional Language Encryption **IX.**

Conclusion:

The data security is major concern in cloud computing , by using this system the data will be secured in multiple levels in order to protect it from hackers as well as from public cloud. The main outcome of this paper is third party has been removed while storing the data into cloud, And if an organizations feels that the intervention of third part required, that will be very minimal because the third part itself does not know how the code book is constructed. The code book is randomly generated. The algorithm implemented here for Encryption and decryption is very well optimized and there by helps in improving the efficiency of the cloud system. **X. Future Enhancement:**

In future as observed in order to reduce the size of the matrix while storing the encrypted data. Data visualization techniques can be used by considering customizable data models. Which will really helps in increasing the security of the data as well as,it helps in increasing the efficiency of the system. Processing the data further use can be made easy with the visualization techniques.

References

[1]. Archana M, MallikarjunShastry P M "A Method for Text Data Fragmentation to Provide Security in Cloud Computing" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019

[2]. Aruna T M, Satyanarayana M S, Divyaraj G N "A Unique Work of Out of Sight Epigraphy Creation for Data Security" Journal of Advanced Research in Dynamical and Control Systems Volume 11 No 7 2019.

[3].MallikarjunaShastry .P.M Abhishek Gaur "Enhanced Approach for Secure Stored Data in Cloud" Test Engineering and Management Volume 83 May 2020.

[4] pJ. Koo, Y. Kim and S. Lee, "Security Requirements for Cloud-based C4I Security Architecture," *2019 International Conference on Platform Technology and Service (PlatCon)*, Jeju, Korea (South), 2019, pp. 1-4, doi: 10.1109/PlatCon.2019.8668963.

[5]. M. Archana P M MallikarjunaShastry "A Review Paper on various Load Balancing Algorithms in Cloud Computing" Vol. 12 Issue 9 2017 P.No. 8579-8585.

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC

[6] A. Arora, A. Khanna, A. Rastogi and A. Agarwal, "Cloud security ecosystem for data security and privacy," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, 2017, pp. 288-292, doi10.1109/CONFLUENCE.2017.7943164.

[7]. M. B. H. Frej, J. Dichter and N. Gupta, "Comparison of Privacy-Preserving Models Based on a Third-Party Auditor in Cloud Computing," 2019 IEEE Cloud Summit, Washington, DC, USA, 2019, pp. 86-91, doi: 10.1109/CloudSummit47114.2019.00020.

[8]. A. E. A. Pacheco, L. M. M. Colaco and S. Desai, "Secure Dynamic Data Storage with Third Party Arbitration in Cloud," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 118-122, doi: 10.1109/ICCONS.2018.8663191.

[9]. Jaydip Kumar "Cloud Computing Security Issues and Its Challenges: A Comprehensive Research" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019

[10]. G. Jain and A. Jaiswal, "Security Issues and their Solution in Cloud Computing", Concepts journal of applied research(CJAR), vol. 02,no. 03, pp. 1-6, 2018.

[11]. A. Hussain, C. Xu, and M. Ali, "Security of Cloud Storage System using Various Cryptographic Techniques," International Journal of Mathematics Trends and Technology (IJMTT), vol. 60, no. 1, pp. 45–51, 2018.

[12]. A. Venkatesh and M. S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," IJSRCSEIT, vol. 3, no. 1, pp. 1741–1745, 2018.

[13]. . K. Subramanian and F. L. John, "Secure and Reliable Unstructured Data Sharing in MultiCloud Storage using the Hybrid Crypto System," IJCSNS, vol. 17, no. 6, pp. 196–206, 2017

[14]. CloudCodes [online] https://www.cloudcodes.com/blog/ dataprotection-controls-techniques.html

[15]. DIGITAL GUARDIAN [online] https://digitalguardian.com/blog/what-cloud-encryption

ISSN: 2233-7857 IJFGCN
Copyright ⓒ2020 SERSC