Encoded Data Methodologies for Cloud Computing Realm's Security Enhancement

Ashutosh Shankhdhar, Arushi Mangla, Prateeksha Chaturvedi

Abstract: ***Cloud Computing has emerged as one of the finest growing technology in today's era with the help of its fundamental services which help in making the capabilities of IT Technology reusable and this is what makes it unique and so popular among the IT enthusiasts. Although along with services being provided, security is also what a user requires to ensure the viability of a system. This paper proposes a feasible mechanism for reliable delivery of services and information and validation of applications of cloud among the data possessor, cloud executive and a client via trusted methodologies. Maintaining confidentiality of the data and secure information is the ultimate aim and focus has also been given on trusted access to the secure data. The objective has been tried to be achieved by devising an algorithm which ensures complete security and reliability of a user's data and information by keeping it secured in a folder, which will then be encoded by the user itself and the key to decode the specific folder will only be with the authorized person. Separate work has been done on the ways by which data will be stored at the Cloud Executive's side, after which the required queries will be implemented to encode the data and then how the authorized resource will be able to decode the folder. This ensures complete reliability of the data at the Cloud Executive's side and also can prove to be very efficient and easy for a user to do so. The proposed mechanism will not only help the users and clients to maintain confidentiality and integrity of their data but also the level of security which may already be provided will also be enhanced and the cloud realm will become more viable for the data possessors too. A secure system will be ensured in the end and that is the end goal today for any person who requests and uses services of the web.***

Index Terms**: *Data Possessor, Cloud Executive, Query Encoding, Folder Decoding.***

I. INTRODUCTION

Cloud Computing is a cross functional approach in which a cloud is a provides services to a user, by giving him access to the data and hardware required, via a Cloud Executive (CE). Some of the operations which take place are – Allocating data at run time, retrieval of data, sharing the resources available. Moreover, the key features and services provided by the cloud computing environment also includes high reliability, very large scale for business practices, on-demand service and low-cost [1]. Since cloud environment offers all these services under one environment, security concerns such as Data Breaching, Insufficient Identity, Insecure Interfaces, and APIs, System Vulnerabilities, Account Hijacking, Data Loss, Denial of Service, Malicious Insiders, Insufficient Due Diligence, Abuse, and Nefarious use of Cloud Services, Advanced Persistent Threats, etc., becomes of major concern here [2]. That is why the need for creating a secure architecture for cloud storage is very important. Confidentiality or security issues in cloud can be dealt by providing an abstraction of the data. It provides the reliability to a user to be ensured that his data is in safe and secure hands. The important services which a user can access in a cloud environment are: core layer, foundation layer, and topmost layer.

A. Core Layer

The core layer serves to provide the main functions, optimality and requirements. It creates a platform for the next two services being provided and provides a visualization and creates a concept on what to do next. It acts as the base layer and generates a platform for services to be put into action. Sharing of parts and applications is also provided by this layer which may include the computer's storing memory, processing system, its functioning power, and everything else which can be provided by a Cloud Resource Sharer.

B. Foundation Layer

The foundation layer provides the area to work upon for the topmost layer in a cloud realm. All types of services and any types of software requested by an end user in a cloud environment can be accessed via a browser over Internet by the PaaS providers, increasing easiness of a user of not requiring to use any kind of service on his server. The main role of this layer comes in when companies with tight budgets need to use these services but with limited resources, then they can do that using this layer and can use their own cloud platform to use and provide sharing and storing of data, without the need of any software requirement from outside. This improves the efficiency and usability of this layer making it easily accessible for all. It is further divided into two layers – Cloud Application Software and Mid Software Foundation of Cloud where the prominent functionalities of the foundation layer are carried out.

Revised Manuscript Received on May 22, 2019

Ashutosh Shankhdhar, Computer Science and Applications, GLA University, Mathura, India.

Arushi Mangla , Computer Science and Applications, GLA University, Mathura, India.

Prateeksha Chaturvedi, Computer Science and Applications, GLA University, Mathura, India.

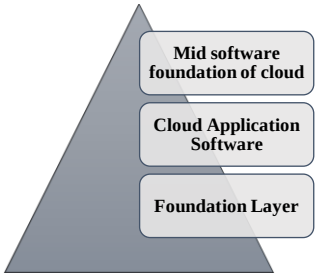

Fig. 1 Further division of Foundation Layer

C. Topmost Layer

The topmost layer of cloud realm, and the functionality and professional working of this layer can be viewed as – It acts like the platform through which a user can communicate with a cloud, and thus it can be viewed as a replication of the interface of a cloud platform.

It is not necessary for this layer to always have an abundant quantity of resources to work upon, even though it is that layer which provides the utilities for a cloud environment. The main components which are required for this layer to work is only a functional PC with a running internet browser.

Cloud has been on a boom since quite some time and has been growing rapidly in many fields since it was born. Also, since in this age there is no assurance of job security or nation's economy, various sectors in industry are realizing the use of this service and how it can prove to be a boon for many. It can provide quick delivery of services and important entities and also give a push to data providers and this can all be achieved at a very minimal rate.

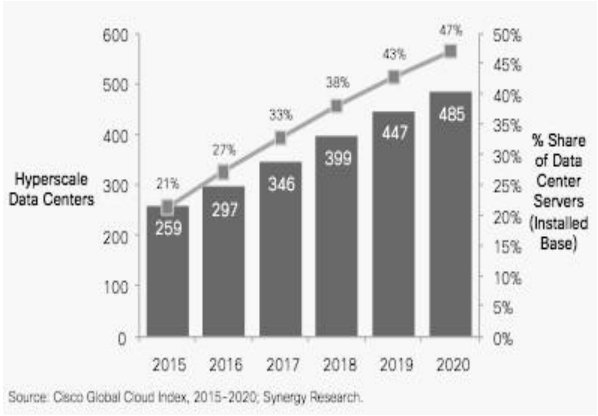

Fig. 2 Market growth in Cloud Environment [8]

Like many other services, the cloud is also threatened by predators and data thieves and thus providing a secure system is becoming necessary in the growing age. Various IT Sectors are placing their trust in the reliable hands of a Cloud Executive and making their information secure becomes of utmost importance.

Since data is being generated at a fast pace and huge information about firms and companies is being placed on cloud, concerns about data-security has come into place, making users to think just how safe and reliable this environment is.

Since cloud computing is an open system architecture, security is of a major concern here. Cloud Computing environment and Cloud itself is sensitive to issues which might come up such as security related to various layers of the network, secure visualization, secure managerial services etc. Confidentiality, Integrity & Authentication are the major problem areas for maintaining security in a cloud environment and this also needs to be maintained by network security. Several algorithms and methodologies have also been proposed for addressing these issues but they were not a great success yet. We have further discussed a very feasible answer for improving security and marinating confidentiality, preventing theft, and making a system more reliable by various methodologies such as data encoding, decoding, and other mechanisms.

II. RELATED WORK

The mechanisms proposed provide enhancement of secure services and information which travels from the Data Possessor (DP) to a client via the Cloud Executive (CE). This is achieved by creation of a folder at DP's end and uploading all the data which needs to be stored and accessed on the cloud in it and then locking it to provide confidentiality and integrity from the Cloud Executive's side. This ensures security of data from unauthorized users or from invaders. This technique is known as Folder locking procedure performed at CE end by DP. This strategy also ensures that another users data remain confidential and no unauthorized user gains its access. The next step is implemented when there is a request from the client's side to provide access to the information requested, and then he gives his credentials and statements regarding the required information to the web portal. This is required to be assured that no data suspicious user to know about the data transaction between CE and DP. The interaction between Cloud Executive and client or a Data Possessor and a client is achieved via the key sharing mechanism. We have relied upon this mechanism as a mode of interaction between a Cloud Executive and client or a Data Possessor and a client as it generates a new security key for every runtime making the system efficient and more secure and trustworthy. Security has been given utmost importance to a cloud storage and environment in this paper, since it has become very essential to for a user to secure his data in this modern age. Also whereas working on a cloud computing environment, there are some patterns or requirements, that can be considered by enterprises when they are approaching data integration within could-based domains [4]. Such as supporting a hybrid cloud, supporting big data, centralized integration platform, ability to empower end user, maximizing reuse, no-code approaches, providing security, governance, and data management, analytics, and predictive intelligenceetc.

Aobing Sun has also discussed a one quantifiable security evaluation system for single or cross cloud platform [3]. That system consists of database, module, scanning engine, recovery engine, evaluation model for defining the security threats & studying aspects of security sets. Also, a Cloud Threat Defense integrated cloud-native scalable solution [2]. It focuses on the endpoint and cloud security control logs for creating a unified security operational tool has also been proposed. In addition to this, Tasnim Kabir & Muhammad Abdullah Adnan have also discussed a security analysis for cloud in which they propose to use secure keys for proper authorization and for secure delivery of the data [5]. Their system guarantees to fulfill the necessary requirements of the major challenges which a user or a Cloud Executive might come across. They are

Correctness, Completeness, and Security. Thus, the focus on improving and greatly enhancing Cloud Computing's security has been of prime concern since long, and has been under study to benefit all the cloud users and to give them a secure interface for sharing and transferring their data in a reliable way. The different key elements of Cloud Security have also been depicted in Fig. 3. All these things are therefore, only motivating a Cloud User to secure his data and ensure a safe transaction to avoid any loss ortheft.

Fig. 3 Faces of Cloud Security [9]

III. DEVISED SYSTEM

Our devised system's primary focus is that there shouldbe a reliable delivering of information among cloud users. A Data Possessor, Cloud Executive, and the Client are the three main cloud users. In Fig. 4 data is being requested by a user from a Data Possessor.

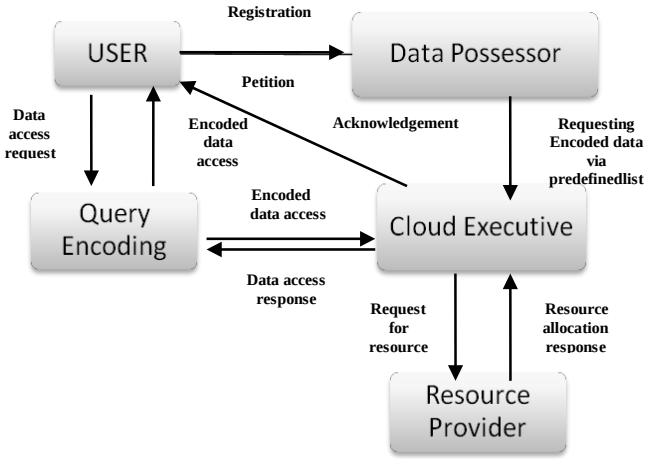

Fig. 4 Data access through Predefined list and Query Encoding

The Data Possessor then first checks the identity of the User and a record in the predefined list for the information requested by the user is created and then a copy of that predefined list is sent to the Cloud Executive. When the appeal is made to the Data Possessor, the Cloud Executive checks the availability of resources from the Resource Provider and then on sufficient availability a confirmation is sent to the client and then when the client again appeals for the information from the Cloud Executive he sends a Request for granting authorized access to the data which is encoded via Request Encoding server and the information request response is sent via the same server.

A new mechanism proposed for enhancing and improving security for the data being reserved in folders is Folder Locking. This has been further described at Cloud Executive's end, pictorially in Fig. 5 in which the data requested by the user is been transmitted on the cloud, and it done by having the CE checking the User Id of each user in the predefined list and then creating a folder and the Data Possessor then sends and syncs the coded and decoded data inside that folder. The folder is then sealed using theunique key of the Data Possessor.

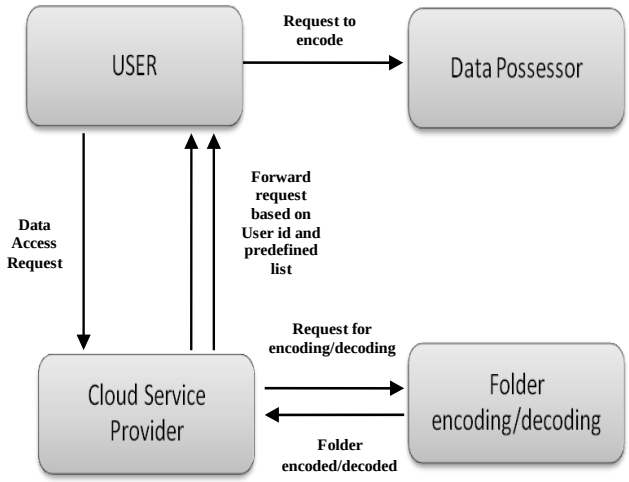

Fig. 5 Folder Encoding by Cloud Executive

The information that the folder has been locked is sent to the user and user will then able to use and access that folder through the key which was previously provided to the Data Possessor. When the data inside the folder needs to be used by the user, the user puts a request inside that locked folder, and then the data can be gained access to, by unlocking that folder through a previously shared key(DP). This gives a user the power to choose the authority and validity of data and with whom he wants to share it.

IV. DEVISED MECHANISM

A number of steps take place in between requesting of data by the user and Data Possessor, and retrieving data from Cloud Executive, such as requesting data from its owner, storing unique ID or data request in a predefined list, encoding data because of confidentiality issues, putting it in the destined folder, locking the folder, and processing the request to provide access to the correct data to the user. Taking all this into consideration, following stated mechanism or steps have been devised accordingly. The steps have further been constructed into three separate algorithms for ease of the Cloud Executive so that each part can be processed more efficiently and be independent of the remaining steps, so that bugs can be detected thus proving to be more reliable functionable and better looking for the Cloud Executive.

A. Mechanism for accumulating data at CE

```
Send the UserID to the DP
for all i in Predefinedlist do
  find UserID in Predefined_i such that UserID = i
  if i = UserID then
    Create a folder for the CE using UserID, FID, RN
    CF field will be checked by in the user request by the DP
    if CF =1 then
      User ← period
      Access to period is gained by D-H key exchange
      Data will be flattened and encoded by DP using confidential key
      CE ← DATA
      DP transmits data to CE in flattened and encoded format on basis
      of UserID
    else
      Uncompressed and decoded data is uploaded on the folder by DP
    end if
  else
    New entry will be generated by DP and also maybe entered in the data
    schema
  end if
end for
```

B. Mechanism for Query Encoding

```
Acknowledgement sent to user through UserID by CE
UserID ← DATA
FID ← DATA
RN ← DATA
Final result is previewed
if HREF is encoded then
  Proceed
else
  Not
end if
Encoded code is sent to CE
Code is decoded
if Code = DataSchema then
  User is allowed to use the folder
else
  Incorrect qualifications are rectified
end if
```

C. Folder Decoding mechanism

```
DP is told by CE that some data is transmitted
User is allowed to access encoded folder
Folder ← decoded
Folder is decoded using confidential key 1
User views the Folder
if Required Data is found adhering to RN then
  if Further Data is encoded then
    It is decoded using nect confidential key 2 shared between DP and
    client
  else
    Direct access of information is provided
  end if
else
  Data not found
end if
```

V. EXAMINATION OF DEVISED METHODOLOGY

A. Confidentiality

The main requirement of security is none other than confidentiality. So in this system, confidentiality has been tried to be balanced between Cloud Executive and Data Possessor. This is achieved by the Cloud Executive not viewing the information of Data Possessor which has been transmitted on the cloud server as it was strongly encoded (secure key & general key encoding) which in turn gives a more secure and reliable platform as compared to any other mechanism as shown in Fig.6.

Security analysis like security against passive attacks, security against active attacks have also been discussed by Jian Shen [7]. Likely they will also be maintained and worked upon once the current algorithm will be completely implemented.

Confidentiality is they key element whereas transferring any data and thus the end user and the Cloud Executive both needs to ensure that the Data Possessor is capable of maintaining its integrity. This proposed mechanism makes sure of that.

Moreover, making a secure server becomes very important for a Cloud Executive when there is a vast amount of data that needs to be stored on the Cloud, and the probability of potential thefts thereby increase. This mechanism can reduce that theft and maintain the integrity of the stored data to a vast extent.

B.Validation and Reliability

The Data Possessor (DP) and Cloud Executive (CE) require validation between them which is achieved via encoded data and predefined list using a unique key of Data Possessor and validation between Cloud Executive and user is given by a Digital Proof.

This validation is required so as to ensure that correct and secured data is being transferred to the correct user across the cloud. This validation of data also needs to be provided to the end user for ensuring that he gets the correct and authorized information

Reliability of data is given by MD5 which acts as a coding mechanism when Data Possessor transmits the information to the Data Manager then code is given by the Data Possessor, replicating the process which was done by Data Possessor for user too. Upon receiving data from the Data Manager, user checks whether the hash matches or not. It accepts the data in case of matching, otherwise communicate to the Data Possessor that the data was interfered with in between. This is how reliability is assured.

Validating and maintaining the integrity of data thus both need to go hand in hand for successful implementation of this algorithm and for maintaining the security at both the Data Possessor's side and at the Cloud Executive's side.

For better performance evaluation we have also taken into account the different algorithms which can be used and assessed by each of their performances to predict which one gives the best performance. It provides a clear picture for a Cloud user to know why the mechanism being used is reliable and ensures safety of data.

Many works done on cloud security and enhancement of the same have tried to protect the integrity and confidentiality of their client's data so that better and reliable service can be provided without the worry of data leakage or unauthorized access to someone else's data on the cloud.

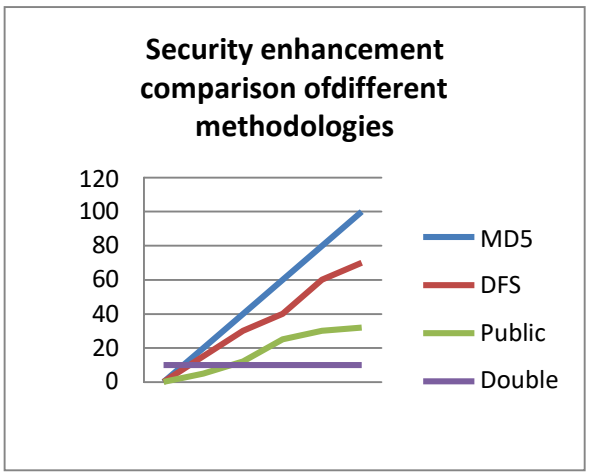

Fig. 6 Comparison between methodologies based on enhancement of security

Improving security enhancement using encoded keys and General key encoding in Fig. 7 have been examined on the context of security level. Strong and efficient performance can be achieved by strong encoding.

C.Capability based Access Control

In our devised system, the authority to for changing and removing the information which is inside the predefined list is with the Data Possessor. All users are classified into the cap list. Horizontal division (row wise) is done in the Access Matrix (AM) for them. Matrix is decided based on the users and not on the basis of the file groups to be used. Following this strategy gives an improved feature because information is frequently used by the designated client as compared to the rest of the clients.

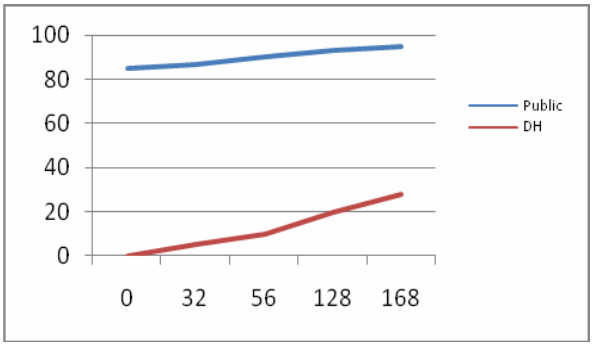

Fig. 7 Comparing performance enhanced by computation on general key and key sharing algorithm

Key encoding can be difficult whereas using general keys as compared to other, which is shown in Fig. 7. This is because key sharing has been used in the devised system between the client and information.

VI. RESULT AND DISCUSSION

All three of the algorithms have been implemented independently so that great efficiency and usability of the mechanism can be achieved for the enhancement of security in securing important and confidential data. Maximum confidentiality and integrity has been tried to be provided to a user along with ensuring correct authorized access to the data. Easiness of a user in securing his data will be increased along with the flexibility to select the authority of his data. The algorithms have been constructed in such a way to create an efficient system by which maximum security can be provided by comparing the reliability and validity with other methodologies and how the level exceeds than the other one. Further modifications and updates have been made keeping that in consideration, and implementation has also been done till a certain level which can ensure the working of the system proposed. Further research and development is also under action and is being worked upon on. A secure system is what a user will gain in the end. In an era of Fog Computing and its legal developments, and other growing technologies using the cloud are being proposed and are under implementation, secure and authorized access to data becomes important for users as well as for cloud service providers for reliable use of theservices [6].

REFERENCES

1. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based On Cloud Storage," 2017 IEEE 3rd International Conference on Big Data Security on Cloud, DOI: 10.1109/BigDataSecurity.2017.12
2. Deepak R Bharadwaj, Anamika Bhattacharya, Manivannan Chakkaravarthy, "Cloud Threat Defense – a Threat Protection and Security Compliance Solution," 2018 IEEE International Conference on Cloud ComputinginEmergingMarkets(CCEM),DOI:10.1109/CCEM.2018.00024
3. Aobing Sun, Guohong Gao, Tongkai Ji, Xuping Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform", 2018 6th International Conference on Advanced Cloud and Big Data, DOI: 10.1109/CBD.2018.00043
4. Davis S. Linthicum, "Cloud Computing Changes Data Integration forever: What's needed right now", 2017 IEEE ComputingSociety.
5. Tasnim Kabir, Muhammad Abdullah Adnan, "A Dynamic Searchable Encryption Scheme for Secure Cloud Server Operation Reserving Multi- Keyword Ranked Search", Department of Computer Science and Engineering, Bangladesh University of Engineering andTechnology.
6. Christian Esposito and Aniello Castiglione, Florin Pop, Kim-Kwang Raymond Choo, "Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective", 2017 IEEE ComputingSociety.
7. Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, Yang Xiang,"BlockDesign-basedKeyAgreementforGroupDataSharinginCloud Computing", 2017 IEEE Computing Society.
8. https://www.ironpaper.com/webintel/articles/forecasting-the-cloud-computing-market-report/
9. https://www.itespresso.it/selezione-del-provider-sicurezza-del-cloud-che-lo-scandalo-nsa-92052.html

AUTHORS PROFILE

Ashutosh Shankhdhar Currently working in GLA University, Mathura as Assistant Professor. He has worked on multiple Technologies such as Cloud, Data Analytics and Machine Learning etc. Currently, He is researching in Cloud Computing Security domain

Arushi Mangla currently pursuing Bachelors of Technology in Computer Science and Applications with specialization in Data Analytics from GLA University. She has worked on technologies such as Machine Learning, Data Mining, Data Visualization, and is currently doing her research on Data Security, Data Warehouse, Super-marts in developing areas.

Prateeksha Chaturvedi currently pursuing Bachelors of Technology in Computer Science and Applications with specialization in Data Analytics from GLA University. She has worked on technologies such as CSS, .net, PHP. She is currently working on Data Science and its Applications.