J. of Ultra Comp. and I.T. Vol. 7(1), 19-26 (2016). ISSN 2229-3531 (Print)
www.compitjournal.org 2455-9997 (Online)

Dynamic Key Based Hybrid Encryption Method for Data Security in Cloud

RAM KINKER SHARMA[1]and M. A. RIZVI[2]

[1]M.Tech CTA NITTTR, Bhoapl (India)
ramkinkar2101@gmail.com
[2]National Institute of Technical Teachers' training and Research, Bhopal (India)
marizv@nitttrbpl.ac.in

(Acceptance Date 10th August, 2016)

Abstract

The concept of Cloud-Computing can offers the framework in order assist the customers efficiently by adding more robust services also by applications via Internet. This type of computing mechanism is increasingly becoming popular as various types of enterprise implementation and data are moving into cloud platforms.In this major hurdle is to spread thisconcept of storage over cloud is shortage of trust among the users of this technology.In this system of cloud can be easily threatened by variouscyber-attacks, because most of the computing mechanisms need tocontain the security approachin order to secure the virtual devices from the attacks.Also thispaper discussed about thesecurity concern of data which is send towards the remote server through channel or internet. By applying the cloud concept within the organizations, there is few security issues may also discussed.

Key words: Data Security, cloud, DES,

I. Introduction

As Green IT has been issued, many companies havestarted to find ways to decrease IT cost and overcomeeconomic recession. The concept of cloud-computing facilities are a newcomputing paradigm in which people only need to pay foruse of services without cost of purchasing physicalhardware. Anideal infrastructure of the information system has been described within the previous researches on the cloud environmentthat may required to be observed as a dynamic change within the concept of thecomputing domains. And this type of computing technique can provide a unique mechanism for applying the computing resources within the business also the user of the companies or by a third partycan use it as the substitute of their computing architecture[1].

The paradigm of cloud-computing may brings along a new IT provisioning model, characterized by keywords likeubiquitous, service-centric, scalable, consumption based and self-services. So the Cloud computing can be referred as an IT deployment model, based on virtualization, where resources, interms of infrastructure, applications and data are deployed via the internet as a distributedservice by one or several service providers. These services are scalable on demand and may also becharged on the basis of pay-per-use basis[2]. This is the idea the cloud computing providersde-scribe to us. However,the security within the cloud environmentis one of the major concerns. IDS approach isamongst the main tools for providing security in networks,cloud and grid.

Cloud enhances collaboration, flexibility, scaling, and availability, and provides the efficient mechanism for decreasing the cost by the effective and the optimal type of computing. Simultaneously, the transformational nature of the cloud is associated along with the important point of security and also the risks of privacy. The rapid emergence of the technology of cloud computing can introduces more of thevulnerabilities.Within this concept the security is considered as the major concern which is referred currently most. When the security aspects have not allowed appropriately for the operations over data and also for transmissions of data then the data is facing the major risk[3]. As the cloud environment can offers the facilitiesfor the various users in order to access and use the data which is stored on cloud then there are chances of the risk of attack over data.Security is considered to be one of the most critical aspects within the cloud-environment because of the confidential andimportant information which isrecorded within cloud area.

The mechanism of Cloud can have the intense capacity of extremely perform re-think and the re-design operations within the organization or business and also within the IT architecture. Within this paper also discussed about the overview of several securityaspects within the cloud environment and also provide some solutions in order to resolve the glitches of security. Since having any type of storage mechanism, some specific type of security features which are required within the cloud system of storage are integrity, confidentiality, write- serializability, read freshness, etc. And these allfeatures may ensure that the data of user is make protected and will never get modified through any unauthorized type of users and also data is used mostly of latest versions if getting retrieved through customers.[3]

This paper aims to demonstrate an innovation for user privacy and the security within thecloud computing type of software. It is accomplished by use of UEC.And also Eucalyptus popular is an open source type of software used fordata security in Cloud which is depends more on the procedures and count measures. So this paper discusses about the issues of data security within the cloud. Some of the issues like privacy andconfidentiality, allocation of data and reallocation, data availability, storage and backup recovery etc.

II. Security Issues:

The mechanism of cloud-computing have found with thevarious opportunities and theissues at the same time. Among the various issues, the issue of security is treated as the most critical bottleneck for the cloud environment for the success of this concept. And issues of security for the cloud-computing techniques arethe dynamic form. Also the location of data is most complicated aspect within the security concept of cloud environment. In this the security only is not an issue but also data privacy challenges existing industries and federal organizations.With the increase in the use of big data in business, many companies are wrestling with privacy issues.

The provider must ensure that the multiple users don't get to see each other'sdata. So, it becomes important to the user to ensure that right security measures are in place andalso difficult to get an assurance that the application will be available when needed[4]. In this study we classify security issues according to fourcategories of the security and the security of data, logical security, physicalsecurity and administrative security.

2.1 Problems of data security :

There are several studies that show the risks which threatened the concept of security of data which is recorded within cloud environment.

2.2 Issue of data confidentiality :

Also another issue is the Confidentiality of the data found within the cloud is also glaring on theaspect of security. An approach of encryption may be used along with thebasic type of approaches. Though, the data in the encrypted form may be protected against the malignant customers whereas privacy feature of the data by the approach of administrator at the service providercannot be keep concealed.

2.3 Issues of Privacy within Cloud :

The current cloud services cause an intrinsic challenge to data privacy[12]. This isbecause they normally result in data being accessible in unencrypted form on amachine operated and owned by dissimilar organization from the data owner.

2.4 Lack of User Control :

User-centric control appears incompatible with the cloud: since a cloudenvironment was used, the service supplier becomes responsible for data storage, ina way which control and visibility is limited[11]. Consumers cannot maintain control over their data when it is processed and stored in the cloud since it isprohibited requirement.

2.5 Unwanted Access :

There needs to be a proper intensity of the access control mechanism within cloud area in order todefend the security of the assets[11]. Cloud computing may really increase thedanger of access to confidential data[13].

III. Data Security and It's TEchniques :

The aspect of security is the major cause in cloud which the various organizations are having their data backupthat is stored over the cloud and also get processed over the cloud area only. The data-security may be different within cloud such as the security for storage, security for computation, security for network *etc*. In this paper describe the way for security to be implemented within the corporate type of network.

3.1 Encrypted-file-systems:

The technique of EFS which is implies for thestoring the encrypted files. This type of encryption processes are familiar to their users and also found over level of file systembut not over the level of application. So these types of approaches are implicitly can apply the techniques of cryptographic for the process of encryptiontherefore the user may saves by performing the complicated work of maintaining the keys within the encryption process. This type of file systems may be applied in order to encrypt data of the client on cloud area. Then this encrypted file is also applied to make encrypted form of data, which is managed and also created the keys that are applied for the encryption process and then decryption process of data[6].

3.2 Ubuntu-Enterprise Cloud:

UEC will aim to solve theabove privacy and the issues of security through ensuring that there is a reasonable balancebetween unrestricted cloud administrators' competence of fulfilling their duties anddisclosure of only the precisely identified information based on administrators[13].

3.3 Trusted Storage System:

Major work of this System is not even recording the data also it may require this storing to be confidential and also should maintain the integrity of data. In order to obtain, the confidentiality of content and alsoits integrity, here applying the techniques of cryptographic that are applied to encrypt the data.

3.4 Authentication within Cloud:

The process of authentication is making sure that correct or valid user is using the data or services. Within the cloud the authentication process maytermed as to ensuring that user or customer is recording the data through providing a authenticated credentials that is the main parameter of authentication approach which implemented. And usershave to prove their identity for the CSPs in order to access different type of data which is recorded over the cloud area. The algorithm of RSA[16] is applied in private cloud and also in the public-cloud thatmay have the various authenticationapproaches.

IV. Data Security Cloud Computing :

With the emergence of internet dependent cloud approaches, this may needs huge focus over the Data Security and also on the Privacy. In this also targeted the Data-loss aspectalso referred as Data-leakage may have adverse affect over the organization, brands and over the trust of the business. And for this provided here the modelfor data security that consists of the authentication process, encryption of data and the integrity of data, recovery, and protectionof user may have also beendeveloped in order toenhance the level of data security within the cloud.

In order confirm the privacy or the data security, the concept of data-protection may be applied as the service. Also in order to prevent the access of the valid data by the invalid user encryption process is appliedover the data in order to enable the data to be not usable and also thenormal type of encryption may by complex to be available. So before performing the data uploadingon the cloud storage, users have to be instructed to authenticate that if data is recorded over the backup machine and also keywords within the files

are not changed.

The process of auditing in cloud is also acomplicated work in order to monitor the compliance of entire policies of securitythrough the clients.The CSP can have the control over the sensitive data of user and also over the processes therefore an automated type of third party mechanism for auditing and for checking the integrity of data is applied and also performed the forensic analysis which is required. And the privacy of thedata among the auditor is also the concept of the security in cloud.

4.1 Confidentiality: confidential is term where the CSPs have also unknown to cloud user data which is uploadedon his own cloud, the cloud storage provider does not learn anyinformation about customer data.

4.2 Integrity: any unauthorized or illegal modification and updating the contents of data of the client through storage in cloud providersmay be detected by the customer whereas maintain the major advantages of the storage service in public cloud.

4.3 Availability: Availability normally defines whether CSP resources are available whenthe customer wants to access them. In addition, we also include durability, which defines whether the data can be recovered by the customer if the data become unavailablefor any reason

4.4 Contractual Security: Finally, CSPs typically provide the SLAwhich governs performance levels and availability. Furthermore, many promiseadditional security guarantees such as restricting the storage data to a certain region or legal jurisdiction or cloud-side encryption of data at rest.

V. Literature REview

In this paper[10] describes about the Mobile Cloud Computing, as a development and extensionof the Cloud-Computing concept and the Mobile-Computing concept is the most growing trend and well accepted technology with fast growth.And given here the combination of theconcept of cloud-computing along with the wireless type of communication infrastructure, portable computing device or the location-oriented services and the mobileetc. has laidthe foundation for the novel computing model. In thispaper given an overview of the Mobile type of Cloud environment architecture that helps the mobile user toconnect their cloud resource within a short time orsearching the resource in a short time.

Within this paper[11] through using previous type of cloud computing technique, the latest trend of LBS concept of spatial service for information in public cloud may also getmodify the actual pattern oflife style, also provided various business facilities.This concept of implementing the cloud-computing techniquehave the developed the geo-spatial dependent data-oriented services and the cloud environment offering the cloudconcept may provide various applications of the spatial type of information along with their applications. In this paper described about the scientific and the technological researches made in the domain of IT and alsomaintain the gap along with the latest trends of the software infrastructure, therefore in order to enhance the establishment of the spatial technology for services and the software.

According to this paper[12] have uses the services of the third-party concept of auditor for monitoring the reliability of cloud server provider. Also it verifies that the data isintact and is responsible for its accountability. In short it deals with the problem of data privacy and its integrity.

Here this paper[13] represented the scheme that describes the use of client fingerprints in order to encrypt the data of users and also again to decrypt while retrieving it.Thealgorithm is a very unique approach as no two persons can have the same fingerprints. Secondly, if this scheme is applied then it'snot always possible that the userby the use of services of cloud may have fingerprint machine and if not then extra money is required topurchase respective machines and to make this model work.

Within this paper[14] suggested an ideal concept of DRMapproach that may protect the key-management-system andalso provides the dynamic control over the usageof the services on cloud. Also, described here the securedmethod for the key management which is dependent over the attribute-oriented method of encryption and also uses the proxyre-encryption process. In this thosecustomers that have the attributesto be fulfilling the policy for accessing the encryptedform of data and alsothat may allow the efficient usage of the rightsmay be capable to regain the key fordata

encryptionand then it again decrypt the data. In this attribute oriented approach may enables the data provider in order to primarily offer the fine-grained mechanism ofaccess control over the data from the group ofusers also this mayoffers the license version of serverto getapplied instant attribute and also it offer the revocation of users.

In this paper[15], discussed about some previous methods of privacy-preserving that satisfiesthe requirement of all the three different parties simultaneously. So in order to refer this problem, here suggested amechanism of retrievable type of data-perturbation and alsoapplied itwithin privacy-preserving of the outsourcing process of data within the cloud environment. This approach may have four differentprocedures. In the first step, an enhanced type of random generatoris suggested in order to produce an appropriate noise.In second step, method of perturbation is applied in order to merge this noise with the actual data. After this process, private details get hide, whereas mean and the covariance of the data that is required by the serviceproviders will keep un-changed. In next step, analgorithm for retrieval is suggested in order toobtain the actual data again from that perturbed form ofdata. In this final stepmerged the retrievable type ofperturbation along with mechanism of access control in order to confirm that only valid customers may get the actual data.

In this paper[16] suggested a latest mechanism of PDP which is termed as theMB-PMDDP, this may helps in outsourcing the multi-copy of thedynamic type of data, in this owner of the data is able to not even archiving but also offer the accessing of data copies that arerecorded by provider of the services of cloud, whereas also enables the updating along with the scaling features of these copies over remotely situated servers.So based on this analysis, the suggested approach is initial step in order to refer the multi-copyof the dynamictype of data. Also it offer the communication in between privileged customerswith the cloud-service-providers which is applied within this approach, in which the valid customers may be efficiently use the copy of data which isobtained from CSP by the use of a secretkey which is shared to the owner also.

According to this paper[17] represented an effective approach of authentication which is applied for the distributed type of mobile-cloud services. In this suggested approach may offer the security along with the support for the mobile users in order to use the more type of mobile based computing services within the cloud which is obtained from various CSPs by the use of aprivate-key. Here also considered the power of securityof the suggested approach which isdependent over the bilinear-pairing concept of cryptosystem and also offer the generation of dynamic nonce. Additionally, thisapproach may helps in mutual authentication process, exchange of keys, and anonymity processalong with the user intractability. By implementing this concept, the verification tables have not needed for SCGtype of trusted services and so this mechanism is applied by variousCSPs.

In this paper[18] researchers have targeted over the various type of situations of the owner of data and also itfragment the users within thesystem among various domains of security which may immensely decrease the complexity of the key management process for the ownersas well as the users of data. And the high degree of the privacy of patient isensured through representing the HMASBE approach. This suggested mechanism may not even assist the compoundtype of attributes because of having the efficient combination of the attribute sets,whereas also this is obtained by the fine-grained mechanism of access control. This suggested approach may help in offering efficient type of on-demand user revocation and also offer attributerevocation along with the break-glass access within some urgent situations.

VI. PROPOSED WORK

This section deals with the proposed work which covers the data security in Cloud Computing environment. This Section main describe about two points of the proposed work:

1. Encryption
2. Decryption

1. START.
2. Read the plain text by the user.
3. Text = Read (message).
4. Read the key of (64 bits) 8 character.
   Key = Read (key)
5. Convert the key into the binary form.
   Skey = StoB (key).
6. Count the number of zeros in skey.
7. while no. of zeros in key = =even
   then

Perform right shift operation key1=skey>>3
Perform Exclusive-or operation key2 = skey XOR key1
Final_Key (128 Bits)=Append (key, key2)
8. Else
Perform left shift operation key1=skey<<3
Perform Exclusive-or operation key2 = skey XOR key1
Final_Key (128 Bits)=Append (key, key2)
9. Divide the plain text into 2 parts 64-64 bits.
PT1=PT(1..64)
PT2=PT(65..128
Divide the final key into 2 parts 64-64 bits
k1=key(1..64)
k2=key(65..128
Perform right shift operation t1 = PT1>>8
Perform Exclusive-or operation t2= PT1 XOR key(1:64)
Perform left shift operation t3 = t2<< 3
Perform left shift operation a1 = PT2<< 8
Perform Exclusive-or operation a2=a1 XOR key(65:128)
Perform right shift operation a3 = a2>> 3
Append the output
Output = t3 + a3
10. Apply the DES algorithm to encrypt and decrypt the data with the help of key.
encryptedData = DES(message).
11. END

Figure 1: Encryption Algorithm

Algorithm for Decryption:
1. START.
2. Read the key for decrytption.
Key = Read (key).
3. Apply the DES algorithm to decrypt the data with the help of key which is used at the time of encryption.
4. decryptedData = DES (encryptedData).
5. Reverse the process and got the real message.
DEC1= decryptedData (1..64)
DEC2= decryptedData (65..128)
Divide the final key into 2 parts 64-64 bits
k1=key(1..64)
k2=key(65..128)
Perform right shift operation t1 = DEC 1>>3
Perform Exclusive-or operation t2=t1XOR k1(1:64)
Perform left shift operation t3 = t2<< 8
Perform left shift operation a1 = DEC 2<< 3
Perform Exclusive-or operation a2= a1 XOR k2(65:128)
Perform right shift operation a3 = a2>> 3
Append the output
Output = t3 + a3
Real message=Convert binary to String BtoS (ouput)
7. END

Figure 2: Decryption Algorithm

This proposed work also deals not only with the encryption technique but also proposed a dynamic approach for key selection. This dynamic approach is describe in following diagrams.

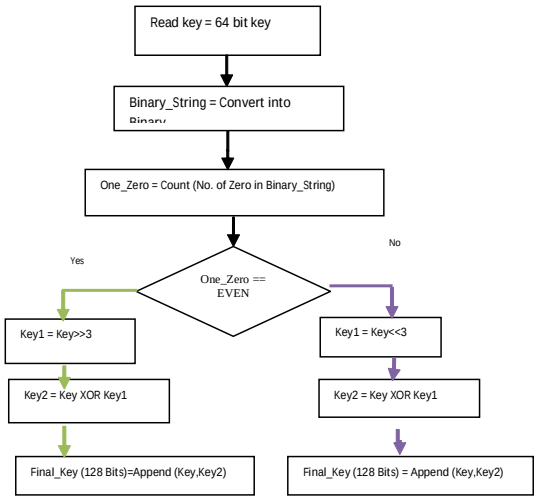

Figure 3: Proposed Dynamic Key Selection

VII. RESULT ANALYSIS

System Configuration

S. No.	Processor	Memory (Primary)	Platform	Software Applica-tion
1	Intel(R) Core(TM)2 Duo CPU	4 GB of RAM	Windows-7 32 bit	JAVA

Text with Key

There are two combination used in evolution of the proposed work over existing work. These two combinations are described in table I and II.

TABLE I: First combination of Texts

	Text	Text
1	Text-1	Bob needs to verify his account

Whereas second combination is presented in table II which is as below:

TABLE II: Second combination of Keys

	Key	Keys Combination
1	Key-1	alicessecretkeys / alicassecretkeys research / rasearch
2	Key-2	bobssecretcommon / bobssacretcommon datasets / datasats

Table III: Avalanche Effect of Proposed Algorithm

Text	**Key**	EXISTING Algorithm	PROPOSED Algorithm
Text-1	Key-1	243	1377
Text-1	Key-2	185	1182

Avalanche Effect :

The avalanche effect denoted to attractive property of cryptographic techniques for data security in cloud, Normally block ciphers techniques technique. The avalanche effect is apparent if, when an input is altered slightly the output alters appreciably. In the case of good-quality block ciphers techniques, such a little change in either the plaintext or the key should cause an extreme alteration should be in the cipher text. It is shown in figure 4.

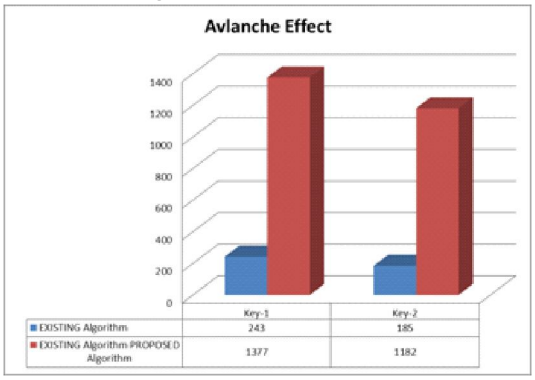

Figure 4: Avalanche Effect Analysis of Proposed Algorithm and Existing works

VIII. Conclusion

This paper is concluded by describing the concepts of Cloud computing which is the form of network of networks established on theinternet, hence there are possibilities of having intrusionsare more along with erudition of the intruder's attacks. Since this environment is conceived service-oriented and many IT services areprovided to customer, service management and delivery of comprehensive architecture for thisenvironment are important. So thisintroduced mechanism has raised the confidentiality level of data and alsointegrity of the stored data. Since the cloud may provides various benefits stillseveral disadvantages are also there within the cloud regionsuch as the down-time, security and some technical problems, this have also more likely to be get affected by various attacks. Therefore in this paper described about some mechanism about the issues in data security along with their solution for data security in could environment.

References

1. S. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: A Multifactor Access Control Framework for Cloud Computing", International Journal of Security and Its Applications, Vol. *7*, no. 2, pp. 15-26 (2013).
2. Arabalidousti, Fatemeh, and Ramin Nasiri. 2013, "Improving IT Service Management Architecture in Cloud Environment on Top of Current Frameworks", The International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC2013). The Society of Digital Information and Wireless Communication.
3. Sapna Malik and M M Chaturvedi (2013),"Privacy and Security in Mobile Cloud Computing", International Journal of ComputerApplications (0975 – 8887) Volume 80 – No 11.
4. Daniela Popa, Marcel Cremene, Monika Borda and Karima Boudaoud, "A Security Framework for Mobile Cloud Applications", published in IEEE 11th Roedunet International Conference, pp. 1-4 (2013) .
5. Ali Newaz Bahar, Md. Ahsan Habib and Md. Manowarul Islam, "Security architecture for mobile cloud computing", International Journal of Scientific Knowledge Computing and Information Technology. Vol. 3, No.3 (2013).
6. Jean-Henry Morin, Jocelyn Aubert and Benjamin Gateau. "Towards Cloud Computing SLA Risk Management: Issues and Challenges", 45th Hawaii International Conference on System Sciences (2012).
7. Ni Zhang Di and Liu Yun-Yong Zhang, "Research on cloud computing security", International Conference on Information Technology and Applications, IEEE (2013).

8. Amin Jula, Elankovan Sundararajan and Zalinda Othman, "Cloud computing service composition: A systematic literature review", Expert Systems with Applications *41*, 3809–3824 (2014).
9. Akhil Behl and Kanika Behl, "An analysis of cloud computing security issues", World Congress on Information and Communication Technologies, IEEE, (2012).
10. Debabrata Sarddar&Ù and Rajesh Bose, "A Mobile Cloud Computing Architecture with Easy Resource Sharing", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161 2014 INPRESSCO.
11. Xing, T.Y., Zhang, S. and Tao, L.F., "Cloud-Based Spatial Information Service Architecture within LBS", Positioning, 5, 59-65. http://dx.doi.org/10.4236/pos.2014.53008 (2014).
12. "Robust Data Security for Cloud while using Third Party Auditor" by Abhishek Mohta, Ravi Kant Sahu and LK Awasthi, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol No. 2, Issue 2, Feb (2012).
13. "Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment" by Varsha Yadav and Preeti Aggarwal in IJCSMC, Vol. 3, Issue. 5, May (2014).
14. HUANG Qinlong 1,2, MA Zhaofeng 1,2, YANG Yixian 1,2, NIU Xinxin 1,2 and FU Jingyi, "Attribute Based DRM Scheme with Dynamic Usage Control in Cloud Computing", China Communications, April (2014).
15. YANG Pan1, 2, GUI Xiaolin1, 2, AN Jian1, 2, YAO Jing1, 2, LIN Jiancai1, and TIAN Feng, "A Retrievable Data Perturbation Method Used in Privacy-Preserving in Cloud Computing", China Communications August (2014).
16. Ayad F. Barsoum and M. Anwar Hasan, "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH (2015).
17. Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", IEEE SYSTEMS JOURNAL, VOL. *9*, NO. 3, SEPTEMBER (2015).
18. CHEN Danwei1, CHEN Linling1, FAN Xiaowei1, HE Liwen1, PAN Su and Hu Ruoxiang, "Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing", China Communications Supplement No.1 (2014).