JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cloud Computing Based Security Enhancement

Versha (Student) Department of Computer Science D.P.G. Institute of Technology and Management, Gurgaon 122001 Gurgaon, India Vershayadav327@gmail.com	Dr Sonal Kanungo (Guide) Department of Computer Science D.P.G. Institute of Technology and Management, Gurgaon 122001 Gurgaon, India Drsonal.cse@dpgitm.com	Mr.Yash Dhankhar(Co-Guide) Department of Computer Science D.P.G. Institute of Technology and Management, Gurgaon 122001 Gurgaon, India yashdhankhardpgitm@gmail.com

ABSTRACT:-Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In the cloud, the data is transferred among the server and client. High speed is the important issue innetworking. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the network layers and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority. Cloud Computing has been selected as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood.

Keywords: ***CloudComputing, Security, File Splitting***

I. INTRODUCTION

Cloud computing mainly provides three kinds of services: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The major difference between service based on cloud computing and traditional service is that user data is stored not in the local server, but in the distributed storage system of the service supplier. In many cases, however, users (especially business users) have high demands regarding data security and reliability. Generally, in traditional data protection methods, plaintext data is stored after encryption. In practical applications, symmetric encryption algorithms, such as DES and AES, are usually adopted because of their efficiency. Although data stored in the cloud server are encrypted, encryption algorithm provides relatively lower security. Therefore, encrypted data are very likely to be vulnerable to attacks and business interests become compromised once the server is invaded. In this project, we propose a secure data storage strategy capable of addressing the shortcomings of traditional data protection methods and improving security and reliability in cloudcomputing.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader

concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just"the cloud", also focuses on maximizing the effectiveness of the shared resources. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

II. LITERATURE REVIEW

PradnyeshBhisikar et al. [1], in this paper, we investigated the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system. In the data transmission proposed, method transferred data is encrypted in the upper-layer on top of the transport layer instead of using IPSec or SSL. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. Webelieve that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. Adding secure cloud storage using the proposed cryptographic solution and with a searchable encryption technique for the files to be accessed, it will work as a betterapproach to the user to ensure security of data. The cloud security using cryptography is already in use for secure data storage which can be enhanced for secure data transmission and storage. An interesting question in this model is if we can construct a scheme to achieve both public verifiability and storage correctness assurance of dynamic data. Besides, alongwith our research on dynamic cloud data storage, we also plan to investigate the problem of fine-grained data errorlocalization.

SajjadHashemi et al. [2], in this we have studied the system of cloud data storage, users store their data in the cloud, so there is noneed to store them locally.Therefore, the security, integrity and availability of data files onstorage distributed cloud servers are guaranteed. To accomplish this, the structure and security solutions of involvedelementsin the process of data storage in the cloud environment should be investigated. About the first element: client; we suggest to use an encryptionmechanism from the customer like AES encryption that its high security and resistance has been proven in many testing. AES has been investigated and analysed by the NIST and its security has been approved by this validated Institute, and this encryption is used to encrypt sensitive information in the United States of America. Also we can use encryption algorithm by means of new methods like genetic algorithm or other dynamic algorithm which security can increase dramatically in this way. The next element must gave special of.The next element must gave special consideration to its security is server,because our data store on the server and we possess storage space virtually as a user. Therefore, the accuracy and availability of data and information retrieval is very important and should provide the necessary security to accomplish this on the server side. Therefore, we use a comparison between some security policies by providers known in the field of providing data storage services, we did the comparison can be clearly seen that in order to the confidentiality of information, some providers use the mechanism of encryption control such as symmetric encryption. About the security of our server recommended service providers in this field to expandandAbout the security of our server recommended service providers in this field to expand and to improve security mechanisms on their servers, because the users of cloud technology will go to the side of those providers that their services have enough security, thus server security will be important and providers can success in this technology with high server security and accountability to the users. The third

element that its security is important in the storage and transmission of data is the connection channel between cloud service providers and user. In our opinion, the most vulnerable point that can put user`s data and information in the cloud environment at risk are communication channel. Because of the Internet and in most cases of the old mechanisms, therefore we must use new methods in order to avoid of unauthorized influences. In this case we can refer to the established protocols and retrieving or establishing more secure transmission channels that they introduce byusing new sciences and methods in the computerscience.

Shah Kruti et al. [3], as we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access controlanddatasecurity.The informationsecuritycanbeeasilyachievedbyusing Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency ofcryptography.

B. Shwetha et al. [4], In this paper, we studied the problem of data security in data storage in cloud servers. To guarantee the correctness of users' data in cloud data storage, we proposed an effectual and flexible scheme with explicit dynamic data support, including block revise, erase, and affix. We use erasurecorrecting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. Our scheme accomplishes the integration of storage correctness insurance and data corruption has been detected during the storage correctness verification across the distributed servers. Our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.We believe that data storage security in Cloud Computing, an area full of challenges and of dominant significance, is still in its infancy to be identified. We envision several possible directions for future research on this area. It allows Third Parity Auditor to audit the cloud data storage without demanding users' time,probability.

III. CHALLENGES IN CLOUD COMPUTING SECURITY

Challenges in Cloud Computing security

The study of cloud computing in recent times is in trend. In today's era, protecting the data is the biggest concern. The possibility of compromised information is creating fear when talking about private, public and hybrid cloud solutions. Some of the organization recruits third-party vendors to manage the data but unauthenticated them of data access.

- Some of the multifaceted challenges for data security on the cloud server:
  - The requirement for protecting data of business and government
  - Multiple occupants are using the same infrastructure for the cloud service model.
  - Legal issues during data mobility.
  - How CSP manages disk space and erases data is also a standard
  - Concern related to auditing, compliance and reporting

- Loss of permeability to key security and functional knowledge that never again is accessible to take care of big business IT security insight and hazard the executives
- A newcomer who can control and view your data but is not a part of your company

Techniques for Protecting Data on the Cloud

A common information security technique is always perimeter-centric and network-centric such as ids and firewalls. But we don't rely totally on these approaches because it does not protect from malicious APIs, privileged users, and other security attacks.

The implementation of encryption techniques must be a robust key management technique that assures that the key being transferred is secure in the network. The crucial part is to audit the entire key management and encryption solution. Encryption works in unity withbasic information defensive techniques. Gathering enhanced security intelligence that presents a complete n-tier method to shielding important information- and reduces the risk of unauthorised access to the data in the cloud.

Hence, it is recommended that CSP must provide encryption techniques,strong access controls, key sharing and key management to prevent unauthorized access to data and provide a high level of security.By performing a multi-layered approach that consists of these critical elements, a CSP can enhance their security condition more adequately and efficiently than by concentrating completely on conventional security methods.

"Use security controls that ensure risky information regardless of where it resides, as point arrangements by their very nature give just restricted permeability," says Tumulak. He stresses that a powerful cloud security arrangement should join three key capacities:

- ✓ Security intelligence
- ✓ Data lockdown
- ✓ Access policies

Strategies for Secure Transition to the Cloud

The basic key to information security is to ensure what is important. Arrangements that empower organizations to unhesitatingly progress to the cloud while as yet utilizing a considerable lot of their conventional framework and speculations offer huge benefits.

Information Security tackles the undertaking cloud security problem by ensuring information within the working climate while setting up security approaches and keeping up with control through a unified administration interface. One key differentiator is that it works with cloud suppliers and undertakings to secure information whether or not it is situated in physical, virtual, or cloud conditions. This design empowers undertakings to control admittance to the factual data, even as the virtual machine relocates to the virtual and cloud world. Associations can build up access approaches and accomplish unlimited information authority in private, public, or mixture cloud conditions.

IV. IMPLEMENTATION AND RESULTS

LoginModule

In computer security, a login or logon or sign in refers to the credentials required to obtain access to a computer system or other restricted area. Logging in or on and signing in or on is the process by which individual access to a computer system is controlled by identifying and authenticating the user through the credentials presented by theuser.

RegistrationModule

In registration get username, email address, password, user generate random verification code. New Random.Next() is used to generate random code. The user can sign in and proceed to next step to verification code. Mail is to user email address by using SMTP protocol. The user can verify the code if verification code is blank then redirect to login page else matched then update user status field with text active and redirect user to the home page.

FTP SettingModule

The proposed system, file get distributed at three different location. First location that is our application and next two more FTP where 2nd and 3rd file is store. In proposed system, we design setting page where this will be further used by application to upload and download file from created table. Insert into table FTP details.

Upload and Downloadmodule

Develop a web interface to upload and download files in cloud storage. The different file uploading links are open. The user can choose the link which we want to upload on cloud. User can upload the file on cloud such as doc file, video, mp3, etc.

File encryption techniquemodule

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itselfprevent interception, but denies the message content to the interceptor.

File decryption techniquemodule

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption.

File splitting and clubbingmodule

In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

SQL HOME PAGE

Fig 1: Connecting To Microsoft SQL Server 2008 R2

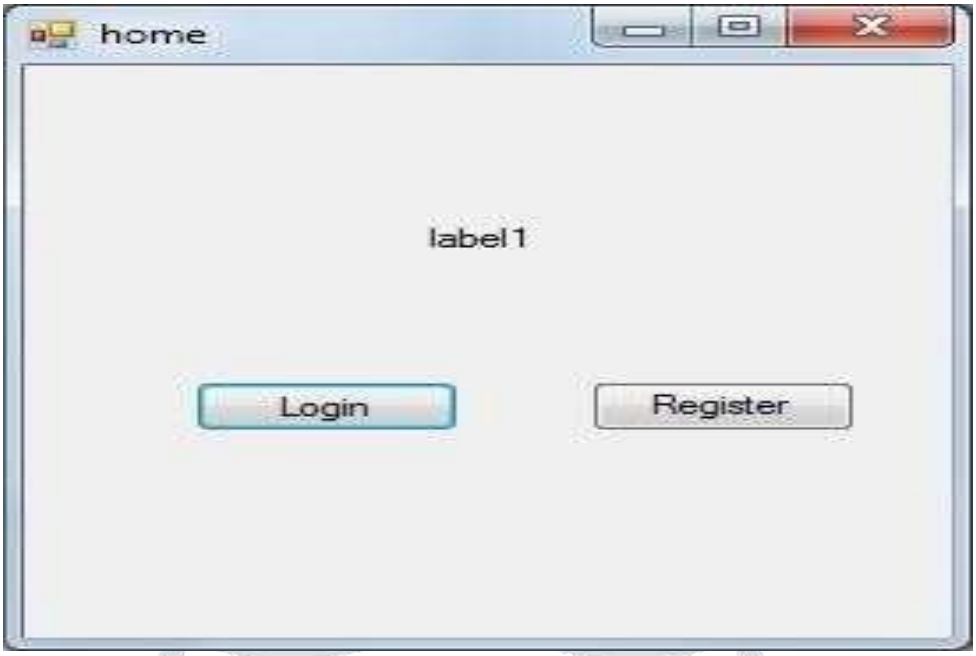

Fig 2: NET Based Applet Screen having Login and Register Button

Fig 3: Registration if you are a new user with your personal details

V. CONCLUSION

As noted in the system of cloud data storage, users store their data in the cloud, so there is no need to store them locally. Therefore, the security, integrity and availability of data-files on storage distributed cloud servers are guaranteed. To accomplish this, the structure and security solutions of involved elements in the process of data storage in the cloud environment should be investigated. About the first element: client; we suggest to use an encryption mechanism from the customer like DES encryption that its high security and resistance has been proven in many testing. Also we can use encryption algorithm by means of new methods like genetic algorithm or other dynamic algorithm which security can increase dramatically in this way. The next element must give special consideration to its security is server, because our data store on the server and we possess storage space virtually as a user. Therefore, the accuracy and availability of data and information retrieval is very important and should provide the necessary security to accomplish this on the

server side. Therefore, we use a comparison between some security policies by providers known in the field of providing data storage services, we did the comparison can be clearly seen that in order to the confidentiality of information, some providers use the mechanism of encryption control such as symmetric encryption.

References

[1] L. Grandinetti, O. Pisacane, M. Sheikhalishahi, "Pervasive CloudComputing Technologies: Future Outlooks and InterdisciplinaryPerspectives", IGI Publication, Advances in Systems Analysis,Software Engineering, and High Performance Computing, ISBN-13:978-1466646834, 2013

[2] G.R. Vijay, A.R.M. Reddy, "Investigational Analysis of SecurityMeasures Effectiveness in Cloud Computing: A Study", ComputerEngineering and Intelligent Systems, Vol.5, No.7, 2014.

[3] P. Mell, T. Grance, "The NIST Definition of Cloud ComputingRecommendations of the National Institute of Standards andTechnology", Special Publication, pp. 800-145, 2011.

[4] A. J. Adoga, G. M. Rabiu, A. A. Audu, "Criteria for Choosing AnEffective Cloud Storage Provider", International Journal ofComputational Engineering Research, Vol.04, Iss.2, 2014

[5] R.A. Popa., J.R. Lorch., D. Molnar., H.J. Wang., and L. Zhuang.,"Enabling Security in Cloud Storage SLAs with Cloud Proof", InUSENIX Annual Technical Conference, Vol. 242, 2011.

[6] Y. Tang., P.P.C Lee., J.C.S Lui., and R. Perlman., "FADE: Secureoverlay cloud storage with file assured deletion", In Security andPrivacy in Communication Networks, Springer Berlin Heidelberg, pp.380-397, 2010.

[7] W. Ren., L. Yu., R. Gao., F. Xiong., "Lightweight andCompromise Resilient Storage Outsourcing with Distributed SecureAccessibility in Mobile Cloud Computing", TSINGHUA Science andTechnology, Vol. 16, No. 5, pp. 520-528, 2011.

[8] X. Dong., R. Li., H. He., W. Zhou., Z. Xue., and H. Wu., "SecureSensitive Data Sharing on a Big Data Platform", TSINGHUA Scienceand Technology, Vol. 20, No. 1, pp. 72-80, 2015.

[9] A. Bessani., M. Correia., B. Quaresma., F. Andre, and P. Sousa.,"DepSky: dependable and secure storage in a cloud-of-clouds", ACMTransactions on Storage (TOS), Vol. 9, No. 4, 2013.

[10] J. Stanek., A. Sorniotti., E. Androulaki., and L. Kencl., "A securedata deduplication scheme for cloud storage", In FinancialCryptography and Data Security Springer Berlin Heidelberg, pp. 99-118, 2014.

[11] B.H. Kim., W. Huang., and D. Lie., "Unity: secure and durablepersonal cloud storage", In Proceedings of the 2012 ACM Workshopon Cloud computing security workshop, pp. 31-36, 2012.

[12] N. Cao., S. Yu., Z. Yang., W. Lou., and Y. T. Hou., "Lt codesbasedsecure and reliable cloud storage service", In INFOCOM,Proceedings IEEE, pp. 693-701, 2012.

[13] S.Murthy., "Cryptographic Secure Cloud Storage Model withAnonymous Authentication and Automatic File Recovery", ICTACTJournal on Soft Computing, Vol. 5, No. 1, 2014.