International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Data protection over multiple cloud using encryption technique

Prof. J. M. Patil[1], Ms. B. S. Sonune[2]

[1]*Assistant Professor Department of Computer Engineering, Shri Sant GajananMaharaj College of Engineering,Shegaon, jaypatil@yahoo.com*
[2]*ME II year Department of Computer Engineering, Shri Sant GajananMaharaj College of Engineering,Shegaon bhagya.sonune@gmail.com*

Abstract - Recent advances have given rise to the popularity and success of cloud computing. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study obtained a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. Malicious user at cloud storage is become most difficult attacks to stop. The proposed research implements the concept of multiple cloud storage along with enhanced security using encryption techniques. Rather than storing complete file on single cloud system. It will split the file in different chunks then encrypt and store them it on different clouds. The Meta data required for decrypting and rearranging a file and it will be stored in metadata management server.

Keywords- Multicloud, security, splitting

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. Subashini and Kavitha [13] argue that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs.Cloud providers should address privacy and security issues as a matter of high and urgent priority.Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards “multiclouds”, “intercloud” or “cloud-of-clouds”[14]. The proposed research implements the concept of multiple cloud storage along with enhanced security using encryption techniques. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed[14].Generally, having a monolithic system run across multiple computers means splitting the system into separate client and server components. In such systems, the client component handled the user interface and the server provided back-end processing, such as database access, printing, and so on [1]. As computers proliferated, dropped in cost, and became connected by ever-higher bandwidth networks, splitting software systems into multiple components became more convenient, with each component running on a different computer and performing a specialized function. This approach simplified development, management, administration, and often improved performance and robustness, since failure in one computer did not necessarily disable the entire system.In many cases the system appears to the client as an opaque cloud that performs the necessary operations, eventhough the distributed system is composed of individual nodes, as illustrated in the following figure[1].

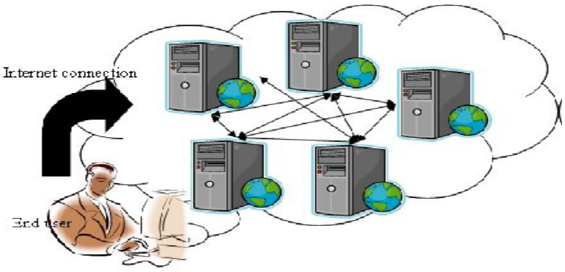


Fig. 1: Architecture of Computing

The capacity of the cloud is maintained because computing operations are invoked on behalf of the client. As such, clients can locate a computer (a node) within the cloud and request a given operation; in performing the operation, that computer can invoke functionality on other computers within the cloud without exposing. The additional steps or the computer on which they were carried out, to the client.
With this paradigm, the mechanics of a distributed, cloud-like system can be broken down into many individual packet exchanges, or conversations between individual nodes.
Traditional client-server systems have two nodes with fixed roles and responsibilities. Modern-distributed systems can have more than two nodes, and their roles are often dynamic. In one conversation a node can be a client, while in another conversation the node can be the server [2][3].

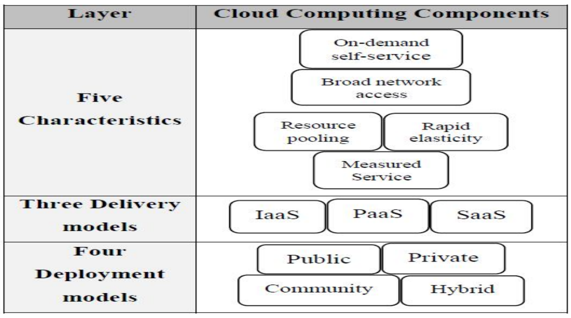
II. LITERATURE REVIEW

Kan Yang and XiaohuaJia propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward security and backward security [2].Cloud computing offer a new and exciting way of computing with various service models that facilitates different services to the users.. Security is an essential parameter and the service provider must ensure that there is no unauthorized access to the sensitive data of an enterprise during the data transmission [6]. Prashant Kumar and Lokesh Kumar are analyzes various security threats to cloud computing[12]. To offering good service, cloud computing service providers must avoid these threats. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE,Luigi Lo Iacono, and Ninja Marnau(Security and Privacy-Enhancing Multicloud Architectures) provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects [1].

III. CLOUD COMPUTING COMPONENTS

The cloud computing model consists of five characteristics, three delivery models, and four deployment models [14]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service [20].

These five characteristics represent the first layer in the cloud environment architecture.The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services.In other words, it is the delivery of computer infrastructure as a service. An example of IaaS is the Amazon web service .In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service.An example of PaaS is GoogleApps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS.



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Fig 2: Cloud Environment Architecture

An example of SaaS is the Salesforce.com CRM application [13],[20]. This model represents the second layer in the cloud environment architecture. Cloud deployment models include public, private, community, and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud) [20]. This model represents the third layer in the cloud environment architecture. There are two types of cloud infrastructure namely private and public clouds. The infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. In particular, this data is out of the user's control, and is managed and shared with unsafe and untrusted servers [14].

IV. SECURITY RISKS IN CLOUD COMPUTING

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment [15]. Users of online data sharing or network facilities are aware of the potential loss of privacy [16]. According to a recent IDC survey [17], the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance [18]. Moving databases to a large data centre involves many security challenges [19] such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha [13] present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources. In different cloud service models, the security responsibility between users and providers is different. According to Tabakiet al. [20], the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data [20]. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [13][14].

V. WHY MOVING TO MULTI-CLOUDS

The migration of cloud computing from single toward multi-clouds to ensure the security of user's data is extremely important.They also suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which leads to different implementations and administrative domains. Recent research has focused on the multi-cloud environment [8], which control several clouds and avoids dependency on any one individual cloud. Moving from single cloud or inner-cloud to multi-clouds is reasonable and important for many reasons. According to Cachin et al. [16] "Services of single cloud are still subject to outage".Vukolic assumes that the main purpose of moving to intercloud is to improve what was offered in single cloud by distributing the reliability, trust, and the security among multiple cloud providers. Furthermore, reliable distributed storage [13] which utilizes a subset of Byzantine fault tolerance (BFT) techniques has been suggested to be used in multi-clouds. A number of recent studies in this area have built protocols for intercloud [8].

VI. IMPLEMENTATION

In proposed system we are implementing the concept of multiple cloud storage along with enhanced security using encryption techniques. We are splits the file in different chunks then encrypt and store it on different cloud. Meta data required for decrypting and rearranging a file will be stored in metadata management server [12].

- Setting up and configuring different cloud server in order to having storage cloud access.Using cloud server API develop file accessing method in different cloud.
- Developing encryption techniques like AES, RSA for file decryption before storing it on cloud.
- Develop a file management classes in dot net.Develop a web interface to upload and download files in cloud storage.

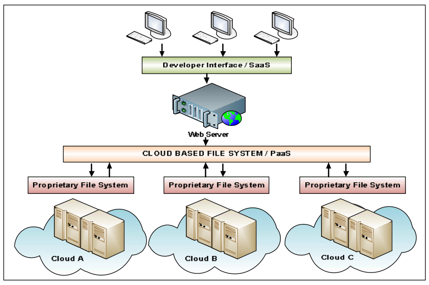


Fig 3: System Architecture

1. File encryption technique design: Setting up and configuring different cloud server in order to having storage cloud access.
2. Remote file split and storing module: Using Cloud Server API develop file accessing method in different cloud.
3. Remote file clubbing module: Developing encryption technique like RSA, AES for file decryption before storing it on cloud.
4. File Management & Web Access Module: Develop a file management classes in dot net.Develop a Web interface to upload and download files in cloud storage.

CONCLUSION

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions.hence by designing the proposed system we are extending the storage cloud security by distributing and encrypting the data.

REFERENCES

[1]J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi-cloud Architectures," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[2]Kan Yang, Ren, XiaohuaJia, Bo Zhang, and RuitaoXie, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IEEE 2013

[3 P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., Sept 2011.

[4]Jing-Jang Hwang and Hung-Kai Chuang, " A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," National Science Council of Taiwan Government, IEEE ,2012

[5]J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.

[6]M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," in Proceeding of IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.

[7]Kan Yang, XiaohuaJia, " Attributed-based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2011

[8]M. A. AlZain, B. Soh and E. Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing," in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing,IEEE,2011

[9]C. Selvakumar G. JeevaRathanam M. R. Sumalatha ," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012

[10]Akash Kumar Mandal, Mrs. ArchanaTiwari , " Performance Evaluation of Cryptographic Algorithms: DES and AES," inProceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science,IEEE 2012

[11]J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D," Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm," in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010

[12]PrashantKumar,Lokesh Kumar," Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 1, December 2013

[13]S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[14]Mohammed A. AlZain, Eric Pardede, Ben Soh , James A. Thom,"Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences,2012

[15]J. Viega, "Cloud computing and the common man",Computer, 42, 2009, pp. 106-108.C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[16]Clavister, "Security in the cloud", Clavister White Paper, 2008H.Mei, J. Dawei, L. Guoliang and Z. Yuan, "Supporting Database Applications as a Service",ICDE'09:Proc. 25thIntl.Conf. on Data Engineering,
2009, pp. 832-843.

[17]C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuringdata storage security in cloud computing",ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication andComputing, 2010, pp. 1-9.

[18]H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Securityand Privacy Challenges in Cloud ComputingEnvironments", IEEE Security&Privacy,8(6),2010,pp