Client and Data Confidentiality in Cloud Computing Using Fragmentation Method

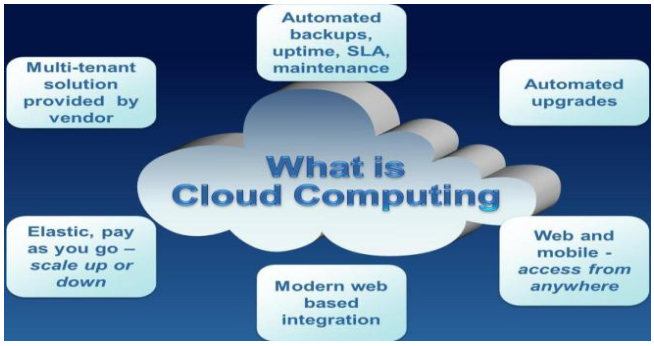
Thota Reshma Kishore, D.Akhila Devi, S.Prathyusha, D.Bhagyasri, Bhuma Naresh

Abstract— In Today's world cloud computing has occupied a prior place in the emerging technologies cause of its ease of access at lower costs. According Moore's Law computer technology, through transistors and integrated circuits, along with digital electronic devices, will double every 18 months to two years. It's a steep curve that began in the 1960s and is expected to continue until about 2020. It is anticipated in the coming years there will be more than one trillion cloud-ready devices, allowing users to work more quickly, conveniently, and at lower cost...this phenomenon presents us with a great risk of data theft and privacy issues. especially for those dealing with sensitive information, Questions that arise include what methods are available and how can that information remain secure to ensure client protection and confidentiality? .Among these Confidentiality privacy is the main reason that many companies and also individuals to some extent are avoiding the cloud ready devices, which also needs be addressed. For this purpose we are proposing a new model that enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This report analyses the challenges posed by cloud computing and the standardization work being done by various standards development organizations (SDOs) to minimize privacy risks in the cloud, including the role of privacy-enhancing technologies (PETs).here the new model to provide confidentiality using fragmentation method The method supports minimal encryption to minimize the computations overhead due to encryption.

***Index Terms— Cloud computing, Data confidentiality,* Fragmentation, Data *outsourcing, Privacy preserving*.**

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.



End users access cloud-based applications through a web browser or a light-weight desktop or mobile_app while the business_software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of infrastructure.

One of the prominent services offered in cloud computing is the cloud data storage, in which; subscribers do not have to store their data on their own servers, where instead their data will be stored on the cloud service provider's servers. In cloud computing, subscribers have to pay the service providers for this storage service. This service does not only provides flexibility and scalability for the data storage, it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time, without any concerns for efficient storage mechanisms and maintainability issues with large amounts of data storage.

Preserving data security is a challenging task because of numerous issues: I) domain specific restrictions, ii) proper implementation of suitable security mechanisms, iii) variation of security measurements among the providers, IV) data aggregation, v) efficient data manipulation, VI) locality restrictions, vii) law restrictions, viii) domain limitations and ix) service level security issues. In Cloud databases, data is stored on multiple dynamic virtual servers across the Cloud. Before being distributed to multiple servers, the data is fragmented. However, usage of pure cryptographic techniques to protect the data can impose heavy computational overheads and also raises key management concerns from the data owner's and provider's point of view. Depending on the application domain, e.g. data used in the IT domain, the user requires the data to be accessible in real time. Therefore, the main focus of our research is directed to preserve confidentiality and privacy while providing efficient accessibility and manageability.

Manuscript received May, 2013.

Thota Reahma Kushiro, Electronics And Computers, K L University, Guntur District, Andhra Pradesh, India.
D.Akhila Devi, Electronics And Computers, K L University, Guntur District, Andhra Pradesh, India.
S.Prathyusha, Electronics And Computers, K L University, Guntur District, Andhra Pradesh, India.
D.Bhagyasri, Electronics And Computers, K L University, Guntur District, Andhra Pradesh, India.

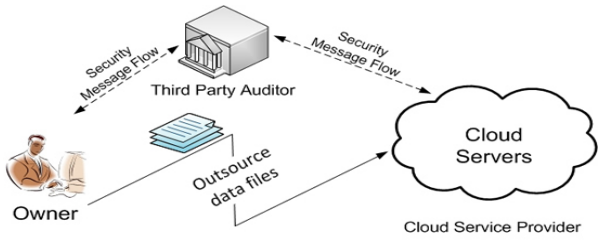
DESIGN:

This paper presents a method for secure and confidential storage of data in the cloud environment based on fragmentation. The method supports minimal encryption to minimize the computations overhead due to encryption. The proposed method uses normalization of relational databases, tables are categorized based on user requirements relating to performance, availability and serviceability, and exported to XML as fragments. After defining the fragments and assigning the appropriate confidentiality levels, the lowest number of Cloud Service Providers (CSPs) is used required to store all fragments that must remain unlink able in separate locations.

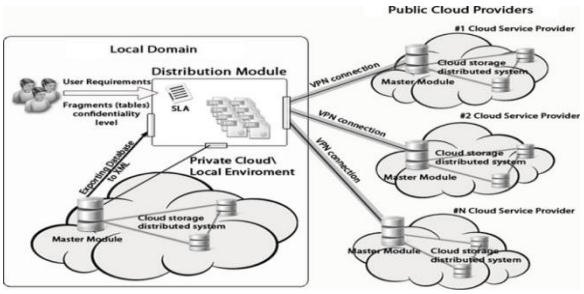
The paper also proposes a methodology to minimize the need for encryption and instead focus on making data entities unlink able so that even in the case of a security breach for one set of data, the privacy impact on the whole is limited. The paper would be relevant to those people whose main concern is to preserve data privacy in distributed systems.

WORK METHODOLOGY:

In this work we observed that, from a customer's point of view, relying upon a solo SP for his outsourced data is not very promising. In addition, providing better privacy as well as ensure data availability, can be achieved by dividing the user's data block into data pieces and distributing them among the available SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block. To address these issues in this paper, we proposed an economical distribution of data among the available SPs in the market, to provide customers with data availability as well as secure storage. In our model, the customer divides his data among several SPs available in the market, based on his available budget. Also we provide a decision for the customer to which SPs he must chose to access data, with respect to data access quality of service offered by the SPs at the location of data retrieval. This not only rules out the possibility of a SP misusing the customers' data, breaching the privacy of data, but can easily ensure the data availability with a better quality of service.



Our proposed approach will provide the cloud computing users a decision model, that provides a better security by distributing the data over multiple cloud service providers in such a way that, none of the SP can successfully retrieve meaningful information from the data pieces allocated at their servers. Also, in addition, we provide the user with better assurance of availability of data, by maintaining redundancy in data distribution. In this case, if a service provider suffers service outage or goes bankrupt, the user still can access his data by retrieving it from other service providers.



Privacy preservation and data integrity are two of the most critical security issues related to user data. In conventional paradigm, the organizations had the physical possession of their data and hence have an ease of implementing better data security policies. But in case of cloud computing, the data is stored on an autonomous business party that provides data storage as a subscription service. The users have to trust the cloud service provider (SP) with security of their data. In, the author discussed the criticality of the privacy issues in cloud computing, and pointed out that obtaining information from a third party is much easier than from the creator himself. Following the pattern of paradigm shift, the security policies also evolved from the conventional cryptographic schemes applied in centralized and distributed data storage, for enabling the data privacy. Many of the cryptographic approaches have been proposed for hiding the data from the storage provider and hence preserving data privacy.

In this authors proposed a scheme in which, the user's identity is also detached from the data, and claim to provide public auditing of data. These approaches concentrate on one single cloud service provider that can easily become a bottleneck for such services. In, the authors studied and proved that sole cryptographic measures are insufficient for ensuring data privacy in cloud computing. They also argued that the security in cloud storage needs a hybrid model of privacy enforcement, distributed computing and complex trust ecosystems. One bigger concern that arises in such schemes of cloud storage services is that, there is no full proof way to be certain that the service provider does not retain the user data, even after the user opts out of the subscription. With enormous amount of time, such data can be decrypted and meaningful information can be retrieved and user privacy can easily be breached. Since, the user might not be availing the storage services from that service provider, he will have no clue of such a passive attack .The better the cryptographic scheme, the more complex will be it is implementation and hence the service provider will ask for higher cost.

CONCLUSION:

From this research work we came to know that, particularly in the cloud databases are sometimes de-normalized (their normal form is decreased to lower level) to increase the performance. Finally with help of all these findings we can provide a high level data confidentiality and security for users and clients.

ACKNOWLEDGMENT

We were very much thankful to our guide Mr.Bhuma Naresh for guiding us and our college K L Universuty for proving us a platform to research on various topics and we are grateful to IJSCE for recognizing our paper and parents and friends for supporting us in every aspect..

REFERENCES

[1] http://www.google.co.in/url?sa=t&rct=j&q=data%20confidentiality%20in%20cloud%20computing&source=web&cd=1&cad=rja&ved=0CC4QFjAA&url=http%3A%2F%2Fwww.ijsi.org%2Fch%2Freader%2Fcreate_pdf.aspx%3Ffile_no%3Di68%26flag%3D1%26journal_id%3Dijsi&ei=94l3UZq8CMLQrQf41ID4Dg&usg=AFQjCNFDlUvfnf_pDv1v1JMPKNZbwwbQ1A&bvm=bv.45580626,d.bmk
[2] http://link.springer.com/chapter/10.1007%2F978-1-84996-241-4_15# page-1
[3] http://www.vmware.com/a/webcasts/details/208
[4] http://scholar.google.co.in/citations?user=waMz0pIAAAAJ&hl=en
[5] http://www.informatik.uni-trier.de/~ley/pers/hd/w/Weippl:Edgar_R=.html
[6] http://en.wikipedia.org/wiki/Cloud_computing_security
[7] http://tempusnova.com/dont-keep-your-eggs-in-one-basket-the-secure-cloud-computing-solution-for-data-protection/
[8]http://technet.microsoft.com/en-us/magazine/jj554305.aspx
[9] http://www.wallstreetandtech.com/technology-risk-management/the-holy-grail-of-cloud-computing-maint/240006774
[10] P. Mahajan et al. Depot: Cloud Storage with Minimal Trust. In USENIX OSDI, 2010.
[11] A.C. Myers and B. Liskov. A Decentralized Model for information Flow Control. In ACM SOSP, 1997.
[12] Survey: Cloud Computing 'No Hype', But Fear of Security and Control Slowing.

THOTA RESHMA KISHORE, Born On 18-02-1992 Pursuing B.TECH at KLUNIVERSITY, Guntur (Dt) Branch: ELECTRONICS AND COMPUTER ENGINEERING Interested in networks, database management systems, Operating systems

D.AKHILA DEVI, Born On 28-07-1992 Pursuing B.TECH at KLUNIVERSITY, Guntur (Dt) Branch: ELECTRONICS AND COMPUTER ENGINEERING Interested in data base management systems, Operating systems, real time systems

S.PRATHYUSHA, Born On 07-07-1992 Pursuing B.TECH at KLUNIVERSITY, Guntur (Dt) Branch: ELECTRONICS AND COMPUTER ENGINEERING Interested in Operating systems, real time systems, data base management systems

D.BHAGYASRI, Born On 22-08-1992 Pursuing B.TECH At KLUNIVERSITY, Guntur (Dt) Branch: ELECTRONICS AND COMPUTER ENGINEERING Interested in data base management systems, Operating systems, real time systems