Data Security in the Realm of Cloud Computing

*Surabhi Jain, **Er. Navneet Randhawa, ***Deepali Kansal
*Student, CSE, A.I.E.T, Faridkot
**Assistant Professor, C.S.E., A.I.E.T., Faridkot
*** Student, CSE, A.I.E.T, Faridkot
Surabhi7117@gmail.com, navneetrandhawa@yahoo.co.in, erdeepali.kansal@gmail.com

ABSTRACT: 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 securitychallenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service [2]. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s) [3]. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

KEYWORDS: Data confidentiality, remote monitoring, Integrity, Source authentication, vulnerability identification and remediation.

The term "cloud" originates from the telecommunications kingdom of the 1990s, when providers began using virtual private network (VPN) services for data communication [1]. VPNs maintained the same bandwidth as fixed networks with considerably "Less cost" these networks supported dynamic routing, which allowed for a balanced utilization across the network and an increase in bandwidth efficiency, and led to the coining of the term "telecom cloud." Cloud Computing and its premise is very similar in that it provides a virtual computing environment that's dynamically allocated to meet user needs.

INTRODUCTION - Cloud computing refers to the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients. The name comes from the use of clouds as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software and computation over a network. It has considerable overlap with software as a service (SaaS) [4].

NEED FOR SECURITY - Most initial computer applications had no or at best very little security. This entertained for a number of years until the importance of data was truly realized. Until then, data was considered useful, but not something to be protected. When computer applications were developed to handle financial and personal data, the real

need of security was felt like never before. People realized that data on computers was an extremely important aspect of modern life.

As many security holes had come by. For example, an intruder can capture the credit card details as they send their information from client to server. If we somehow protect this transit from an intruder's attack, it still does not solve our problem.

Once the merchant receives the credit card details and validates them so as to process the order and later obtain the payments, the merchant stores the credit card details into its data base. Now any attacker can simply succeed in attacking that database and gain access to all the credit card numbers stored therein.

There are many security issues for cloud computing as it engulfs various technologies including Networks, database, transaction management, concurrency control, dynamic load balancing and many others. These many issues are a matter of serious concern for the cloud as well.

For E.g., A network that interconnects the system has to be secure, confidential and free from modern attacks. Moreover, data mining techniques may be applicable to malware detection in clouds.

In this paper we will discuss only on some of the aspects regarding security issues of cloud computing. One such architecture is to efficiently store data in foreign machines [5]. Another is to query encrypted data as much of data could be encrypted on the cloud [6].

This architecture facilitates that this data can be protected and only given access to the Authorized Individuals. This amounts to the Secure Third Party Publication of data that is mandatory for data outsourcing as well as external publication.

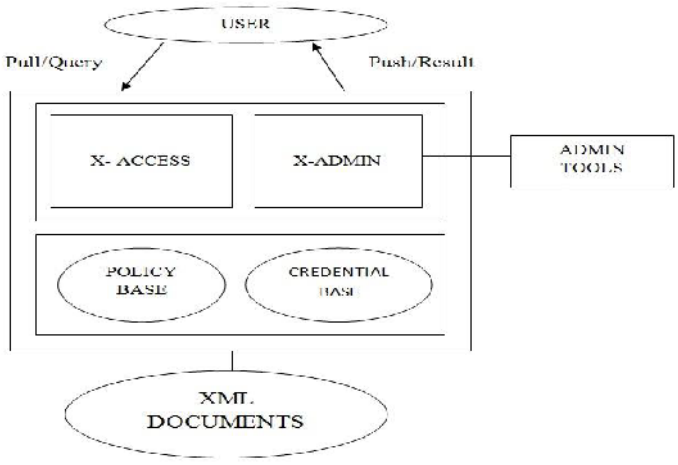

Fig 1. Access Control Framework

Key Aspects:

In this mechanism the security policy is specified depending upon user roles and credentials.

Users must possess those credentials to have access to all the XML documents.

The credentials depend upon their roles.

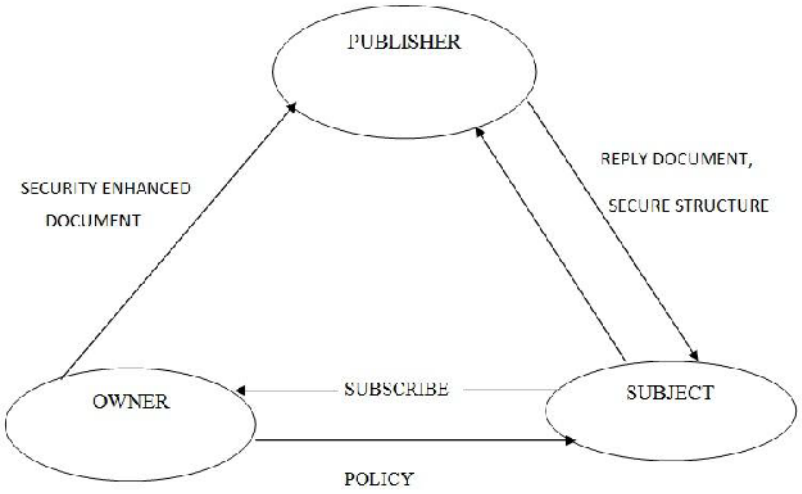

Fig 2. Security Regarding Third Party Publication

Key Aspects:

In this architecture if access is granted to the roots, it does not necessarily mean access to all the child nodes.

Thus, access will be restricted to certain portions of the document only so limited access could be granted.

Thus, with the help of XML [7], these roles can be restricted.

APPLICATION- Security is key issue in the wireless data transmission which is prone to threats like data loss like eavesdropping, unauthorized modification, false value, repeated information, etc. Thus, providing security, confidentiality, integrity, authentication non-repudiation, availability is to be maintained which would ensure that data is in safe hands and has been received or transmitted through secure channel.

HOW DOES IT WORK

The basic idea is to have untrusted third party publishers.

The owner of the document specifies access control policies for the given subject.

These subjects guide the policies from the owner when they subscribe to a document. Now the publisher will apply the policies relevant to the subject and give portions of the document to the subject.

Now, since the publisher is untrusted, it could also give false implication and information to the subject.

Thus, the owner will now encrypt the various combinations of the document and policies using his/her private key [8].

Thus, with the help of Merkle signature [9] and encryption techniques, the subject can verify the authenticity and completeness of the document.

Here, in Cloud atmosphere, the third party publisher is that machine that stores that sensitive data in the cloud. This data has to be protected with these techniques and thus completeness can be ensured as well as maintained.

CONCLUSION - In this paper, we have proposed a new frame work of cloud computing. We have focused on security aspect of web services of cloud computing and we have not discussed the integration of our proposed security mechanism with other components of Hadoop [10] and Apache [11]. We intend to do so in our forthcoming endeavors.

FUTURE WORK- This architecture can be used to provide security in hospitals, in reservation systems, on line ticketing system using cloud. It can be also implemented in ATM machines where a person remotely logs in into his/her account using cloud computing.

REFERENCES

[1] Cong Wang, Qian Wang and Kui Ren.―Ensuring Data Storage Security & Communication in Cloud computing 978-1-4244-3876-1/2009 IEEE.

[2] A. Sahai, S. Graupner, V. Machiraju, and A. van Moorsel. Specifying and monitoring Quality of Service in commercial grids through sla. pages 292 _ 299, May 2003.

[3] Borja Sotomayor, Kate Keahey, and Ian Foster. Combining batch execution and leasing using Servers & virtual machines. pages 87 96, Boston, MA, United states, 2008.

[4] How Web-hosted Software-as-a-Service (SaaS) Lowers the Total Cost of Ownership (TCO) for Electronic Access Control Systems, http://www.brivo.com/benefits/cost,

[4] Software as a Service : http://en.wikipedia.org/wiki/Software_as_a_ service

[5] Muys, A. (2006). Building an Enterprise- Scale Database for Foreign Machines.

[6] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS'05, 2005.

[7] Bertino, E, et al, Access Control for XML documents, Data and Knowledge Engineering, Volume 43, #3, 2002

[8] T. Elgamal. A Private Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In Advances in Cryptology – CRYPTO '84, number 196 in LNCS, pages 10–18. Springer, 1985.

[9] On the security and the efficiency of the Merkle signature scheme, Technical Report 2005/192, Cryptology ePrint Archive, 2005. Available at http://eprint.iacr.org/2005/192/.

[10] HADOOP: http://hadoop.apache.org; http://hadoop.apache.org.core/docs/r0.18.3/h dfsdesign.html

[11] Zhang, K. (2009). Adding user and service-to-service authentication to Hadoop. Retrieved from https://issues.apache.org/jira/browse/HADO OP-4343.