

Chapter 56

A Randomized Cloud Library Security Environment

A. V. N. Krishna

PujyaShri Madhavanji College of Engineering & Technology, India

ABSTRACT

Cloud computing is leading the technology development of today's communication scenario. This is because of its cost-efficiency and flexibility. In Cloud computing vast amounts of data are stored in varied and distributed environments, and security to data is of prime concern. RSA or Elliptic Curve Cryptography (ECC) provides a secure means of message transmission among communicating hosts using Diffie Hellman Key Exchange algorithm or ElGamal algorithm. By having key lengths of 160 bits, the ECC algorithm provides sufficient strength against crypto analysis and its performance can be compared with standard algorithms like RSA with a bit length of 1024 bits. In the present work, the plain text is converted to cipher text using RSA or ECC algorithms. As the proposed model is intended to be used in Cloud environment, a probabilistic mathematical model is also used. While the data is being retrieved from the servers, a query is being used which uses the mathematical model to search for the data which is still in encryption form. Final decryption takes place only at user's site by using the private keys. Thus the security model provides the fundamental security services like Authentication, Security, and Confidentiality to the transmitted message and also provides sufficient strength against crypto analysis in Cloud environment.

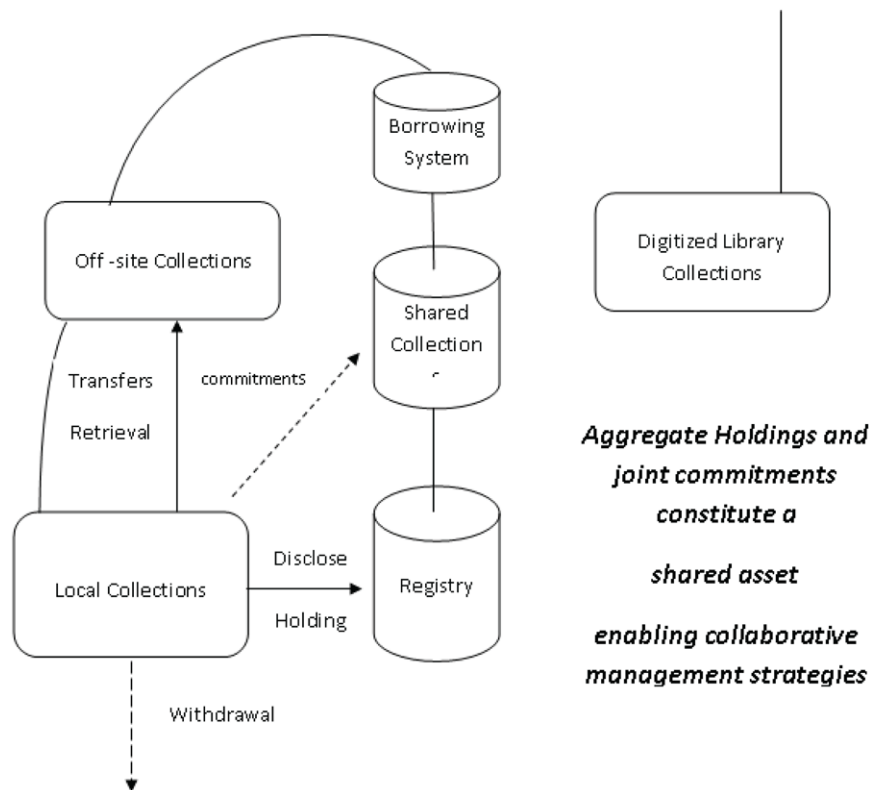
INTRODUCTION

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 use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams (see Figure 1). Cloud computing entrusts remote services with user's data, software, and computation.

Today many of the largest software companies operate almost entirely in the cloud, the top five software companies by sales revenue all have major cloud offerings, and the market as a whole is predicted to grow at a very fast pace. Yet, despite the trumpeted business and technical advantages of cloud

DOI: 10.4018/978-1-5225-8176-5.ch056

Figure 1. Cloud computing environment



computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud.

Mell and Grance (2012) define the “security” concerns that are preventing companies from taking advantage of the cloud as:

- Traditional Security
- Availability
- Third-Party Data Control

Traditional Security

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company.

Availability

These concerns center on critical applications and data being available. Well-publicized incidents of cloud outages include G mail, Amazon.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-randomized-cloud-library-security-environment/224623

Related Content

Recent Advances in Edge Computing Paradigms: Taxonomy Benchmarks and Standards for Unconventional Computing

Sana Sodanapalli, Hewan Shrestha, Chandramohan Dhasarathan, Puviyarasi T. and Sam Goundar (2021). *International Journal of Fog Computing* (pp. 37-51).

www.irma-international.org/article/recent-advances-in-edge-computing-paradigms/284863

A Stable Matching Algorithm for VM Migration to Improve Energy Consumption and QOS in Cloud Infrastructures

Abdelaziz Kella and Ghalem Belalem (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 606-623).

www.irma-international.org/chapter/a-stable-matching-algorithm-for-vm-migration-to-improve-energy-consumption-and-qos-in-cloud-infrastructures/119874

Social Implications of Big Data and Fog Computing

Jeremy Horne (2018). *International Journal of Fog Computing* (pp. 1-50).

www.irma-international.org/article/social-implications-of-big-data-and-fog-computing/210565

Necessity of Key Aggregation Cryptosystem for Data Sharing in Cloud Computing

R. Deepthi Crestose Rebekah, Dhanaraj Cheelu and M. Rajasekhara Babu (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 1393-1407).

www.irma-international.org/chapter/necessity-of-key-aggregation-cryptosystem-for-data-sharing-in-cloud-computing/224638

Development of Community Based Intelligent Modules Using IoT to Make Cities Smarter

Jagadish S. Kallimani, Chekuri Sailusha, Pankaj Lathar and Srinivasa K.G. (2019). *International Journal of Fog Computing* (pp. 1-12).

www.irma-international.org/article/development-of-community-based-intelligent-modules-using-iot-to-make-cities-smarter/228127