International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 7229-7234

http://www.ripublication.com

Ensuring Security in Cloud Computing Using Biometric Schemes

V.Subapriya[1] and E.Thenmozhi [2]

[1]Student /Department of Computer Science,

Sathyabama University Chennai, India

Email: subapriyarajesh@gmail.com

[2]Assistant Professor,

Faculty of Computing, Sathyabama University, Chennai, India

Email: rajthenu@gmail.com

ABSTRACT

Cloud computing is said to be as big datacenters where information stored in it are distributed worldwide and can be accessed by anyone at anytime and anywhere. Security is one of the major issues with information stored in public/private cloud. Biometric authentication scheme and pattern recognition is used to ensure security with the information stored in cloud.

Keywords: Cloud computing, Biometric authentication, Pattern recognition.

1. INTRODUCTION

Maintaining secure information in cloud is a major problem faced nowadays, however there are many security schemes and algorithms used to ensure secure access of data present in cloud. Identity based encryption is considered to be least preferable scheme to ensure security since it is easily prone to code breaking attacks and private keys are decrypted without any authorization. This modern biometric authentication scheme in combination with pattern recognition overcomes all hindrance and produces more security than other schemes implemented already.

In proposed scheme, two-level authentication is used where first level is considered to be as pattern recognition and second level is considered to be as biometric authentication which can be in the form of iris recognition, finger prints, voice recognition etc. These patterns and biometric features are given as an input for accessing the data stored in cloud.

2. BIOMETRIC AND ITS CHARACTERISTICS

The term biometric came from a Greek word ‘bios’ means life and ‘metrics’ means measurement. Biometric means unique physiological characteristics which are used for authentication of an individual. It is also defined as differentiable and resistant characteristics of an individual.

3. RELATED WORKS

[1] The existing system which is used for cloud security uses identity based encryption which is insecure and prone to code breaking attacks like password attacks and man in middle attacks and also identity based encryption system cannot be used for non-repudiation. Identity based encryption rely on cryptographic techniques that are insecure against code breaking attacks.

[2] Security scheme using 768 bit RSA modulus also faces some difficulty and complexity for quantum computer. It is known as complexity classes which

contain the integer factorization problem.

[3] Generalized role based access control scheme for securing applications in cloud computing is not a complete security solution itself. It is just an access control model which is useful in the real world, but in future we need to explore these integrations issues and build a prototype based on generalized role based access control.

DRAWBACKS OF EXISTING SYSTEM

1. Inconsistent results: The recognition of individuals using identity based encryption is not the same at all conditions. Sometimes it is poor and prone to some code breaking attacks.
2. Accuracy and data availability: Due to insecurity access of data present in cloud, data availability, integrity, accuracy and consistency of data is major drawback with the existing system which can be overcome using two-level biometric authentication scheme in proposed system.

4. PROPOSED SYSTEM

The scope of this work is to provide a secure access of data present in public/private cloud. A two-level biometric authentication scheme is used in which first level authentication is done using pattern recognition like circle, triangle, square etc. Second level authentication is done with unique biometric features like iris, fingerprints, voice matching with that of feature template stored in the system. Sample biometric features are shown below.

Figure 1. Representation of data

SYSTEM MODEL

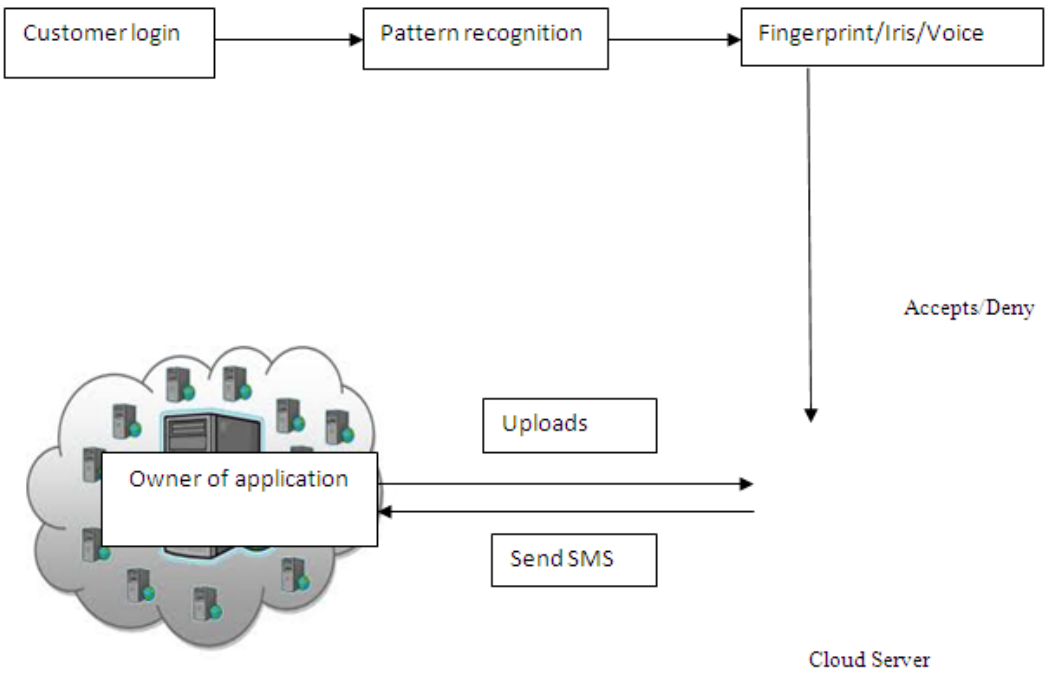

Figure 2. Architecture Diagram

5. CONCLUSION

Cloud computing internet based infrastructure which provides client with data storage and service on demand, to design a secure data access approach for cloud computing and its client is a main aim of efficient cloud computing. In this paper I have proposed a scheme called two-level biometric authentication which provides a secure access of application present in cloud. Thus proposed system is developed with numerous advantages.

REFRENCES

[1] A.Shamir, "Identity-based cryptography and signature schemes", Advances in cryptography, CRYPTO'84, Lecture notes in Computer Science, Vol.196,pp.47-53,1985.

[2] Kleinjunget al., "Factorization of a 768-bit RSA modulus", V1.0.IACR ePrint archive, Jan. 7, 2010.

[3] M.J.Moyer, M.Ahamad, "Generalized role-based access control",proc. Of IEEE Int'l Conf. on Distributed Computing Systems ICDSC2001), Mesa, .391-398, 2001.

[4] P. Boss, Mllladi et al., "Cloud computing- The blue cloud project",www.ibm.com/developerworks/websphere/zones/hipods/, Oct. 2007.

[5] http://aws.amazon.com/. 2010-09-08.

[6] http://code.google.com/intl/zh-CN/appengine/. 2010-10-15.

[7] http://hadoop.apache.org/. 2010-10-20.

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009.

[9] J. Girard and J. Pescatore, "Teleworking in cloud: Security risks and services"- A Gartner Report, May 15, 2009.

[10] J. Viega, "Cloud computing and the common man", IEEE Computer Magazine, pp.106–108, Aug. 2009.

[11] Yaoxue Zhang, Yuezhi Zhou, "A new cloud operating system: Design and implementation based on transparent computing", ActaElegtronicaSinica, Vol.39, No.5, pp.985–990, May 2011.(in Chinese)