Chapter 43
Cloud and Cyber Security Through Crypt-Iris-Based Authentication Approach

Sherin Zafar
Jamia Hamdard University, India

ABSTRACT

In today's world, wireless technology utilized by cloud and cyber technology has become an essential part of each and every user. Sensitivity, authentication and validation needs to be looked upon. Traditional technologies using simple encryption and password mechanisms cannot look upon the security constraints of today's cyber world; hence, some better authentication aspects like biometric security utilizing most strong feature like iris are exploited in this chapter to serve as specific secure tool.

INTRODUCTION

Due to the various intrinsic vulnerabilities present in cloud computing, cyber world and various wireless networks, the prime concern for users is the attainment of various secure parameters in form of authentication, integrity of their data present all across, non-repudiation and confidentiality of the various contents spread across the cloud along-with trust management and accessing the control for performing secured peer-to-peer conveyance over a cloud network. Therefore, security, routing and Quality of Service (QOS) are critical issues, that require immediate research attention due to the dynamic, unpredictable nature of most networks and also as they vary from each other greatly from the viewpoint of the area of application. This chapter specifies different attacks, parameters and methods of securing networks, followed by concepts of biometrics, and CIBA (Crypt Iris Based Authentication) approach. This chapter specifies different attacks, parameters and methods of securing networks, followed by concepts of biometrics, and CIBA (Crypt Iris Based Authentication) approach.

DOI: 10.4018/978-1-5225-8176-5.ch043

Security Challenges in Cloud Networks

The conventional cloud networks utilized across the cyber world are dependent upon some of the specific features that include contentment, organization tread and negligible dependency on a permanent architecture. A large number of security restrictions occur in modern day cloud world irrespective of their unique features that include distributed framework, coercive topologies, concerted and undistinguished wireless connectivity, compassed battery power, memory requirements and reckoning power capabilities. Occurrence of attacks from either direction is the major security consideration which is faced by modern day wireless cloud networks indifferent to fixed wired networks therefore each node in such type of networks should accoutre any attack coming from any direction accurately and diffusely. Due to malignant property each node shouldn't trust any node instantaneously. Distributed architecture of any cloud network is preferred over a centralized one due to various security restrictions that lead to various damages due to structure infirmity. A large number of attacks like the black hole, neighbour, worm-hole, denial of service, message betrayal, hastening, jellyfish, byzantine, blackmail etc. which affects cloud security.

Parameters and Methods for Securing a Cloud

Guerin and Orda (1999) have specified authentication, non-repudiation, confidentiality, integrity and availability as some of the most important security goals of MANET which are discussed below:

- **Authentication:** A mobile network before starting communication with a peer node authenticates it to ensure its identity. Not performing authentication can cause unauthorised access, as the attacker can impersonate the node and thus, access sensitive resources and information by interfering with the working of various other nodes of the network.
- **Non-Repudiation:** Non-repudiation is very important for detecting and isolating compromised nodes of various networks, by ensuring message originality of the specified sender and receiver without any denial.
- **Confidentiality:** Maintaining confidentiality is quite important for various military, strategic and sensitive applications, as it ensures non-disclosure of information to unauthorised entities.
- **Availability:** It is also one of the key security goals of MANET, as it ensures that services in a network operate properly by avoiding failures even in case of denial-of-service attack.
- **Integrity:** Integrity specifies accuracy of data. It ensures accurate and correct information to be transmitted across the various nodes of the network. There are many conventional methods for securing a wireless cloud network and a cyber world which are described below.

Key and Trust Management

Basic security supporting element for any system comes from a hybrid of asymmetric and symmetric cryptosystems, referred as key and trust management. Key management includes key exchange and key updating by maintaining authentication, confidentiality, integrity and non repudiation. Trust management leads to building of a trust graph where various nodes (entities) in a mobile network to their respective edges are specified through verifiable credentials. Below are discussed some very important services of key management: