World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:10, 2015

Multimodal Biometric Cryptography Based Authentication in Cloud Environment to Enhance Information Security

Authors : D. Pugazhenthi, B. Sree Vidya

Abstract : Cloud computing is one of the emerging technologies that enables end users to use the services of cloud on 'pay per usage' strategy. This technology grows in a fast pace and so is its security threat. One among the various services provided by cloud is storage. In this service, security plays a vital factor for both authenticating legitimate users and protection of information. This paper brings in efficient ways of authenticating users as well as securing information on the cloud. Initial phase proposed in this paper deals with an authentication technique using multi-factor and multi-dimensional authentication system with multi-level security. Unique identification and slow intrusive formulates an advanced reliability on user-behaviour based biometrics than conventional means of password authentication. By biometric systems, the accounts are accessed only by a legitimate user and not by a nonentity. The biometric templates employed here do not include single trait but multiple, viz., iris and finger prints. The coordinating stage of the authentication system functions on Ensemble Support Vector Machine (SVM) and optimization by assembling weights of base SVMs for SVM ensemble after individual SVM of ensemble is trained by the Artificial Fish Swarm Algorithm (AFSA). Thus it helps in generating a user-specific secure cryptographic key of the multimodal biometric template by fusion process. Data security problem is averted and enhanced security architecture is proposed using encryption and decryption system with double key cryptography based on Fuzzy Neural Network (FNN) for data storing and retrieval in cloud computing . The proposing scheme aims to protect the records from hackers by arresting the breaking of cipher text to original text. This improves the authentication performance that the proposed double cryptographic key scheme is capable of providing better user authentication and better security which distinguish between the genuine and fake users. Thus, there are three important modules in this proposed work such as 1) Feature extraction, 2) Multimodal biometric template generation and 3) Cryptographic key generation. The extraction of the feature and texture properties from the respective fingerprint and iris images has been done initially. Finally, with the help of fuzzy neural network and symmetric cryptography algorithm, the technique of double key encryption technique has been developed. As the proposed approach is based on neural networks, it has the advantage of not being decrypted by the hacker even though the data were hacked already. The results prove that authentication process is optimal and stored information is secured.

Keywords : artificial fish swarm algorithm (AFSA), biometric authentication, decryption, encryption, fingerprint, fusion, fuzzy neural network (FNN), iris, multi-modal, support vector machine classification
Conference Title : ICCSI 2015 : International Conference on Computer Science and Innovation
Conference Location : Chicago, United States
Conference Dates : October 08-09, 2015