عنوان مقاله:

Implementation of hybrid cryptographic schemes in a cloud environment for enhanced medical data security

محل انتشار:

مجله آنالیز غیر خطی و کاربردها, دوره 12, شماره 2 (سال: 1400)

تعداد صفحات اصل مقاله: 16

نویسندگان:

- - - Department of Computer Science, VISTAS, Chennai, India.

- - - Department of Computer Science, VISTAS, Chennai, India.

خلاصه مقاله:

Nowadays, several security architectures in cloud computing were employed in several applications, but they failed to secure the cloud data entirely. The current approaches use the ensemble algorithm for the decryption and encryption purpose to enhance the security technique. The input medical dataset is usually raw and might contain redundant packets and missing values. Initially, the data is preprocessed by means of the normalization technique. By using Enhanced Principal Component Analysis (EPCA) method, various attributes of the data can be obtained. After the extraction process, the classification mechanism is carried out for recognizing the attacks. The attack is predicted and is classified by means of the Adaptive AlexNet CNN classifier algorithm. A hybrid cryptographic technique in a cloud environment for improving the security rate and providing privacy preservation of the medical data in the cloud environment is presented. The proposed work mainly concentrates mostly on implementing hybrid cryptographic schemes which include AES algorithm, enhanced honeypot algorithm, SHA۳ hashing and OTP in the cloud environment. It enhances the security of the data to a great extent. Thus, the presented technique is secured effectively that makes the intruders difficult to access the system as they need to attain control over servers.

کلمات کلیدی:

cloud computing, encryption, decryption, Enhanced Principal Component Analysis, Adaptive AlexNet CNN classifier, cryptographic technique, enhanced honeypot algorithm, SHA۳ hashing and OTP

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1561217