World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:8, No:08, 2014

Security of Database Using Chaotic Systems

Authors : Eman W. Boghdady, A. R. Shehata, M. A. Azem

Abstract : Database (DB) security demands permitting authorized users and prohibiting non-authorized users and intruders actions on the DB and the objects inside it. Organizations that are running successfully demand the confidentiality of their DBs. They do not allow the unauthorized access to their data/information. They also demand the assurance that their data is protected against any malicious or accidental modification. DB protection and confidentiality are the security concerns. There are four types of controls to obtain the DB protection, those include: access control, information flow control, inference control, and cryptographic. The cryptographic control is considered as the backbone for DB security, it secures the DB by encryption during storage and communications. Current cryptographic techniques are classified into two types: traditional classical cryptography using standard algorithms (DES, AES, IDEA, etc.) and chaos cryptography using continuous (Chau, Rossler, Lorenz, etc.) or discreet (Logistics, Henon, etc.) algorithms. The important characteristics of chaos are its extreme sensitivity to initial conditions of the system. In this paper, DB-security systems based on chaotic algorithms are described. The Pseudo Random Numbers Generators (PRNGs) from the different chaotic algorithms are implemented using Matlab and their statistical properties are evaluated using NIST and other statistical test-suits. Then, these algorithms are used to secure conventional DB (plaintext), where the statistical properties of the ciphertext are also tested. To increase the complexity of the PRNGs and to let pass all the NIST statistical tests, we propose two hybrid PRNGs: one based on two chaotic Logistic maps and another based on two chaotic Henon maps, where each chaotic algorithm is running side-by-side and starting from random independent initial conditions and parameters (encryption keys). The resulted hybrid PRNGs passed the NIST statistical test suit.

Keywords : algorithms and data structure, DB security, encryption, chaotic algorithms, Matlab, NIST
Conference Title : ICCTA 2014 : International Conference on Computing : Theory and Applications
Conference Location : London, United Kingdom
Conference Dates : August 21-22, 2014

Open Science Index, Computer and Systems Engineering Vol:8, No:08, 2014 publications.waset.org/abstracts/9108.pdf