IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, June 2025
Impact Factor: 7.67

Improving Digital Forensic Security: A Secure Storage Model with Authentication and Optimal Key Generation Based Encryption

Dr Khaleel UR Rahman Khan[1], Ch. Praneetha[2], K. Suhas[3], P. Vamshi krishna[4], A. Pavan Teja[5]
Professor & Dean (Academics) [1]
Student, Computer Science and Engineering[2,3,4,5]
ACE Engineering College, Ghatkesar, India.

Abstract: *Abstract secure storage model for digital forensics represents essential progress in the domain, addressing the major problems associated with protecting and maintaining digital evidence. This method employs recent encryption systems and optimal key generation methods to ensure the confidentiality and integrity of data throughout the investigative process. Cloud forensics is an intelligent development of digital forensics to be preserved against online hacking. But, centralized evidence gathered and preservation reduces the reliability of digital evidence. This architecture integrates numerous modules and methods to address the exclusive tasks modeled by cloud computing (cc) environments in the framework of forensic investigations. This paper develops a new digital forensic architecture utilizing the authentication with optimal key generation encryption (dfa aokge) technique. The main intention of the dfa-aokge method is to use a bc-distributed design to allocate data between numerous peers for data collection and safe storage. Additionally, the dfa-aokge model uses the secure block verification mechanism (sbvm) for the authentication procedure. Also, the secret keys can be produced by the usage of the enhanced equilibrium optimizer (eeo) model. Furthermore, the encryption of the data takes place using a multikey homomorphic encryption (mhe) approach and is then saved in the cloud server. The simulation value of the dfa-aokge methodology takes place in terms of different aspects. The simulation results exhibited that the dfa-aokge system shows prominent performance over other recent approaches in terms of different measures.*

Keywords: In encryption, decryption digital forensic architecture, multikey homomorphic encryption