x +
/Desktop/phd/Current%20work/Paper/accepted%20paper/published%20paper%202.pdf
Read aloud | Ask Copilot | 1 of 28

Enhancing Cloud Forensic Investigation System in Distributed Cloud Computing Using DK-CP-ECC Algorithm and EK-ANFIS

Shaiqa Nasreen[1,2,*] and Ajaz Hussain Mir[1]

[1]*Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar, J & K, India*
[2]*Islamic University of Science and Technology, Awantipora, J&K, India*
E-mail: shakks10@outlook.com; ahmir@rediffmail.com; ahmir@nitsri.net
**Corresponding Author*

Received 29 March 2022; Accepted 25 August 2022;
Publication 15 February 2023

Abstract

The investigation as well as recovery of data gathered as of digital devices associated with computer crime is involved in Digital Forensics (DF). In a distributed Cloud Server (CS), DF investigation is more complicated (during collecting, preserving, and reporting the evidence) as well as insecure during gathering evidence as of the cloud sources. Centered on the DF investigation system, numerous works were performed. However, lots of challenges still remain that bring about cybercrime. The work developed a robust cloud forensic investigation system centered upon distributed Cloud Computing (CC) for conquering the challenges. It is framed into the '3' phase (i.e.) originally, Group Key Generation (GKG) phase that enables the authorized user to upload or download the evidence for maintaining the evidence's trustworthiness. Distributed Key Cipher Policy Elliptic Curve Cryptography (DK-CP-ECC) algorithm performed the Secure Data Transfer (SDT) phase. It aids in maintaining the evidence's privacy together with confidentiality. Exponential Membership Function Adaptive Neuro-Fuzzy Interference System (EK-ANFIS) carries out the CS selection with the aid of a deer hunting