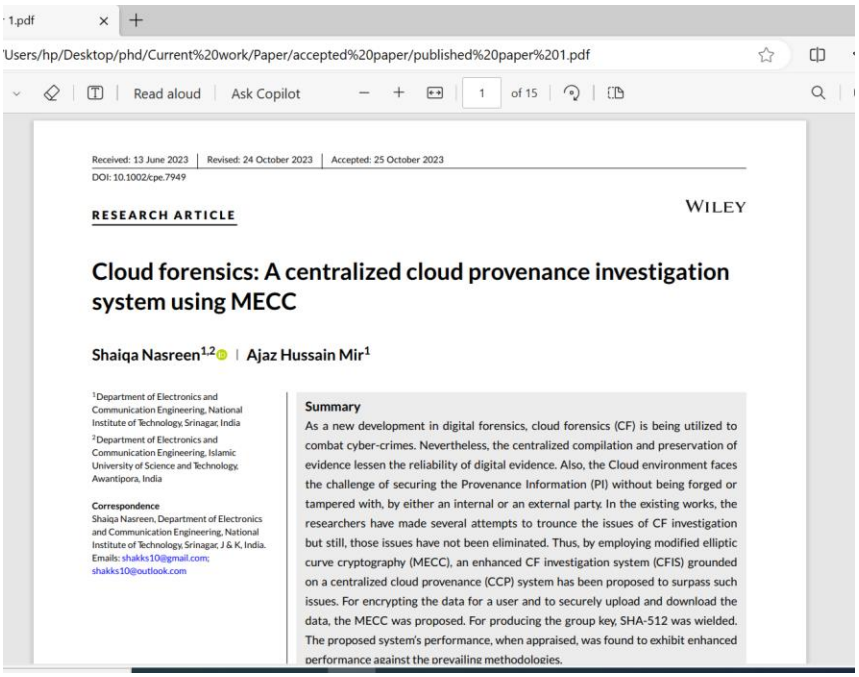

Received: 13 June 2023 | Revised: 24 October 2023 | Accepted: 25 October 2023
DOI: 10.1002/cpe.7949

RESEARCH ARTICLE

WILEY

Cloud forensics: A centralized cloud provenance investigation system using MECC

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

[1]Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar, India
[2]Department of Electronics and Communication Engineering, Islamic University of Science and Technology, Awantipora, India

Correspondence
Shaiqa Nasreen, Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar, J & K, India.
Emails: shakks10@gmail.com; shakks10@outlook.com

Summary

As a new development in digital forensics, cloud forensics (CF) is being utilized to combat cyber-crimes. Nevertheless, the centralized compilation and preservation of evidence lessen the reliability of digital evidence. Also, the Cloud environment faces the challenge of securing the Provenance Information (PI) without being forged or tampered with, by either an internal or an external party. In the existing works, the researchers have made several attempts to trounce the issues of CF investigation but still, those issues have not been eliminated. Thus, by employing modified elliptic curve cryptography (MECC), an enhanced CF investigation system (CFIS) grounded on a centralized cloud provenance (CCP) system has been proposed to surpass such issues. For encrypting the data for a user and to securely upload and download the data, the MECC was proposed. For producing the group key, SHA-512 was wielded. The proposed system's performance, when appraised, was found to exhibit enhanced performance against the prevailing methodologies.