Read publisher preview | Download citation | Copy link

Article | Publisher preview available

# De-centralized information flow control for cloud virtual machines with hybrid AES-ECC and improved meta-heuristic optimization based optimal key generation

January 2023 · International Journal of Intelligent Robotics and Applications 7(4):1-20

January 2023 · 7(4):1-20

DOI:10.1007/s41315-022-00268-6

**Authors:**

To read the full-text of this research, you can request a copy directly from the authors.

Citations (1) References (36) Figures (13)

Abstract and Figures

Cloud computing is now used by many enterprises due to its increased computational efficiency, economic effectiveness, as well as flexibility. However, security is currently the main issue impeding the cloud computing platform's growth. Therefore, Decentralized Information Flow Control (DIFC) has been proposed as a suitable remedy for resolving the cloud security problems. Using conventional network access and encryption technology was not practicable in the DIFC to effectively restrict the spread of the tenant's personal data inside the system. Therefore, a novel DIFC framework for cloud virtual machines (VM) is suggested here. The suggested system encapsulates four entities such as central authority (CA), encryption proxy (EP), cloud server (CS), and cloud tenant VM. The EP has implemented the ciphertext data-flow security technique. Encryption is carried out using the newly proposed hybrid “Advanced Encryption Standard (AES)–Elliptic Curve Cryptography (ECC) algorithm”. The hybrid AES-ECC encryption technique uses the proposed Improved Poor Rich Optimization (IPRO) model to compute the optimal key. The implementation of the developed work is evaluated against the existing works for the "Chess, T1014D100K, and Retail datasets”. In particular, for the T1014D100K dataset, the cost function of the suggested model at the 2.5th iteration is 57.14%, 62.05%, 80%, 54.2%, and 56% better than the old models like BOA, SMO, SSA, PRO, and LA correspondingly.




General structure of the selected… | An illustration of the decentraliz… | ECC based encryption | AES based encryption… | Proposed hybrid AES-ECC…

Figures - available from: International Journal of Intelligent Robotics and Applications

This content is subject to copyright. Terms and conditions apply.

Discover the world's research

- 25+ million members
- 160+ million publication pages
- 2.3+ billic citations

Join for free

Sponsored videos

Read publisher preview Download citation Copy link

A preview of this full-text is provided by Springer Nature.
Learn more

Content available from International Journal of Intelligent Robotics and Applications
This content is subject to copyright. Terms and conditions apply.

International Journal of Intelligent Robotics and Applications (2023) 7:406–425
https://doi.org/10.1007/s41315-022-00268-6

REGULAR PAPER

# De-centralized information flow control for cloud virtual machines with hybrid AES-ECC and improved meta-heuristic optimization based optimal key generation

**Yogesh B. Gurav**[1] · **Bankat M. Patil**[1]

Received: 9 November 2021 / Accepted: 24 November 2022 / Published online: 13 January 2023
© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2023

## Abstract

Cloud computing is now used by many enterprises due to its increased computational efficiency, economic effectiveness, a well as flexibility. However, security is currently the main issue impeding the cloud computing platform's growth. Therefore Decentralized Information Flow Control (DIFC) has been proposed as a suitable remedy for resolving the cloud security prob lems. Using conventional network access and encryption technology was not practicable in the DIFC to effectively restrict th spread of the tenant's personal data inside the system. Therefore, a novel DIFC framework for cloud virtual machines (VM is suggested here. The suggested system encapsulates four entities such as central authority (CA), encryption proxy (EP) cloud server (CS), and cloud tenant VM. The EP has implemented the ciphertext data-flow security technique. Encryptio is carried out using the newly proposed hybrid "Advanced Encryption Standard (AES)–Elliptic Curve Cryptography (ECC algorithm". The hybrid AES-ECC encryption technique uses the proposed Improved Poor Rich Optimization (IPRO) mode to compute the optimal key. The implementation of the developed work is evaluated against the existing works for the "Chess T1014D100K, and Retail datasets". In particular, for the T1014D100K dataset, the cost function of the suggested mode at the 2.5th iteration is 57.14%, 62.05%, 80%, 54.2%, and 56% better than the old models like BOA, SMO, SSA, PRO, an LA correspondingly.

**Keywords** Cloud computing · DIFC · Hybrid AES-ECC model · IPRO algorithm

## Abbreviations

| | |
|---|---|
| AES | Advanced encryption standard |
| AOPF-SFS | Attribute-order-preserving-free-SFS |
| AT-DIFC+ | Adaptive trust-aware decentralized information flow control |
| BFA | Brute force attack |
| BOA | Butterfly optimization algorithm |
| CA | Central authority |
| CS | Cloud server |
| DIFC | Decentralized information flow control |
| ECC | Elliptic curve cryptography |
| EP | Encryption proxy |
| IFC | Information flow control |
| IPRO | Improved poor rich optimization algorithm |
| KPA | Known-plaintext attack |
| LA | Lion algorithm |
| OBL | Opposition based learning |
| PRO | Poor rich optimization algorithm |
| RSA | Rivest–Shamir–Adleman cryptosystem |
| SFS | Sort-filter-skyline |
| SMO | Spider monkey optimization |
| VM | Virtual machines |
| SSA | Salp Swarm algorithm |
| TLC-IFC | Tenant-led ciphertext information flow control |

## 1 Introduction

Recently, clo
every sector
puting resou
sive basis (B
2015). One
is data secu
their private

✉ Yogesh B. Gurav
ybgurav1977@gmail.com

[1] Department of Computer Science & IT, Dr.Babasaheb Ambedkar Marathwada University, Aurangabad, MS, India

Read publisher preview Download citation Copy link

Citations (1) References (36)

**Defensive Strategies Against PCC Attacks Based on Ideal (t,n)-Secret Sharing Scheme**

Article

Sep 2023

View

Read publisher preview Download citation Copy link

Recommended publications Discover more

Conference Paper

Two-Fold Improved Poor Rich Optimization Algorithm based De-centralized Information Flow Control for...

January 2022

Read more

Chapter

State of the Art on Cloud-Information Flow Control

January 2022

Users lose responsibility for personal information whenever they upload their data to the Cloud. The growth of cloud computing would be hampered if indeed the cloud environment fails to produce an appropriate security mechanism to ensure data security. Throughout the intervening decades, access control and encryption methods were unable to properly restrict the spread of private tenant data ... [Show full abstract]

Read more

Article Full-text available

Data Flow Management and Compliance in Cloud Computing

August 2015 · IEEE Cloud Computing

Jatinder Singh · Julia Powles · Thomas Pasquier · Jean Bacon

As cloud computing becomes an increasingly dominant means of providing computing resources worldwide, legal and regulatory issues associated with the cloud also become more pronounced. In particular, there is a heightened focus on ensuring the privacy and integrity of end-users' personal data. At present, the cloud is opaque, a black-box. The technical means for enforcing and demonstrating ... [Show full abstract]

View full-text

Article Full-text available

A New Cryptosystem for Secured Data Communications in Plagiarism Checking Process Using Blockchain T...

October 2022 · Wireless Personal Communications

S. Anirudh · R. Shaan Sundar · Ganapathy Sannasi

Blockchain technology is playing a major role in the process of providing security to the data of different kinds of applications. This technology is considered the verified document of every transaction. Proof of Low Infringement and Plagiarism is a consensus mechanism designed to revolutionize heavy identity, asset tracking, and academic participation. Research articles and innovations are not ... [Show full abstract]

View full-text

Download on the App Store GET IT ON Google Play

Company
About us
News

Support
Help Center

Business solutions
Advertising
Recruiting

Read publisher preview Download citation Copy link

© 2008-2024 ResearchGate GmbH. All rights reserved. Terms Privacy Copyright Imprint Consent preferences