Document details

Proceedings - 2nd East Indonesia Conference on Computer and Information Technology: Internet of Things for Industry, EIConCIT 2018
November 2018, Article number 8878629, Pages 18-23
2nd East Indonesia Conference on Computer and Information Technology, EIConCIT 2018; Novotel HotelMakassar; Indonesia; 6 November 2018 through 7 November 2018; Category numberCFP18JVB-ART; Code 153210

Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms (Conference Paper)

Salma[a] ✉ Olanrewaju, R.F.[a] ✉ Abdullah, K.[a] ✉ Rusmala[b] ✉ Darwis, H.[b] ✉

[a]Electrical and Computer Engineering, International Islamic University, Kuala Lumpur, Malaysia
[b]Faculty of Computer Engineering, Cokroaminoto Palopo University, Palopo, Indonesia

Abstract

View references (10)

Cloud computing is an IT model that offers a large number of storage space, unbelievable computing power and inconceivable speed of calculations. There are a number of costumers like corporate components, social media programs and individual customers are all moving towards to the vast area of cloud computing. The importance of cloud computing comes out with the security of data accessibility, reliability and reliability of information. The verification and permission is more necessary to access information as 'cloud' is only assortment of actual super computer speed through the world. There are many research has been done on security of file encryption with AES algorithm. There is no any successful attack yet against AES but because of a higher increasing of cybercrime it could be possible attack on it like brute force attack and algebraic attack. Hence, in this research has been proposed a hybrid structure of Dynamic AES (DAES) and Blowfish algorithms. This procedure specifies the security of uploaded file on the cloud with a strong encryption method and also the privacy and reliability of submitted information of a user with considering performance of speed. © 2018 IEEE.

SciVal Topic Prominence ⓘ

Topic: Revocation | Encryption | Diffie-Hellman

Prominence percentile: 99.255 ⓘ

Author keywords

AES | Blow fish | cloud computing | DAES | encryption | Hybrid algorithm | security

Indexed keywords

Engineering controlled terms:	Cloud computing · Data privacy · Differential equations · Digital storage · Reliability
Engineering uncontrolled terms	Advanced Encryption Standard · Brute-force attack · DAES · Encryption algorithms · Hybrid algorithms · Individual customers · Reliability of information · security
Engineering main heading:	Cryptography

Metrics ⓘ View all metrics >

1 Citation in Scopus
36th percentile

PlumX Metrics
Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 1 document

Cloud computing performance analysis strategy to enhance the QOS for imminent it sector

Madavi, B. , Vijayakarthik, P. , Sheshappasheshappa, S.N.
(2020) Journal of Advanced Research in Dynamical and Control Systems

View details of this citation

Inform me when this document is cited in Scopus:

Set citation alert >

Set citation feed >

Related documents

The survey of various techniques & algorithms for SMS security

Karale, S.N. , Pendke, K. , Dahiwale, P.
(2015) ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems

RGB Component Encryption of Video Using AES-256 Bit Key

Geetha, N. , Mahesh, K.
(2020) Lecture Notes on Data Engineering and Communications Technologies

Implementing information security mechanism over cloud network

Bharathan, T. , Santhosh Kumar, B.J.

ISBN: 978-153868048-3
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/EIConCIT.2018.8878629
Document Type: Conference Paper
Volume Editors: Haviluddin H.,Wibawa A.P.,Purnawansyah P.,Riza L.S.,Azis H.,Salim Y.,Malani R.,Gaffar A.F.O.,Darwis H.,Astuti W.,Fattah F.,Satra R.,Herman H.,Hasanuddin T.,Manga A.R.
Publisher: Institute of Electrical and Electronics Engineers Inc.

(2019) International Journal of Recent Technology and Engineering

View all related documents based on references

Find more related documents in Scopus based on:

Authors > Keywords >

References (10)

View in search results format >

□ All | Export | Print | E-mail | Save to PDF | Create bibliography

□ 1 Gupta, R.
(2013) *Enhanced Security for Cloud Storage Using Hybrid Encryption*, 2 (7), pp. 2710-2713. Cited 9 times.

□ 2 Gajra, N.
(2014) *Private Cl Loud Security: Secured User Authenticatio on by Using Enhanced Hybrid Algorithm*

□ 3 Sachdev, A.
(2013) *Enhancing Cloud Computing Security Using AES Algorithm*, 67 (9), pp. 19-23. Cited 35 times.

□ 4 Jadhav, S.P., Nandwalkar, P.B.R.
(2015) *Efficient Cloud Computing with Secure Data Storage Using AES*, 4 (6), pp. 2-6.

□ 5 Arora, R., Parashar, A.
(2013) *Secure User Data in Cloud Computing Using Encryption Algorithms*, 3 (4), pp. 1922-1926. Cited 61 times.

□ 6 Nithyabharathi, P.V., Kowsalya, T., Baskar, V.
(2014) *To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES*, 3 (2).

□ 7 Thakur, J., Kumar, N.
(2011) *DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis*, 1 (2), pp. 6-12. Cited 116 times.

□ 8 Singhal, N., Raina, J.P.S.
(2011) *Comparative Analysis of AES and RC4 Algorithms for Better Utilization*, pp. 177-181. Cited 58 times.

□ 9 Salama, D., Elminaam, A., Mohamed, H., Kader, A., Hadhoud, M.M.
(2010) *Evaluating the Performance of Symmetric Encryption Algorithms*, 10 (3), pp. 213-219. Cited 2 times.

□ 10 Li, J., Zhang, Y., Chen, X., Xiang, Y.
Secure attribute-based data sharing for resource-limited users in cloud computing
(2018) *Computers and Security*, 72, pp. 1-12. Cited 243 times.
doi: 10.1016/j.cose.2017.08.007
View at Publisher

< Back to results | 1 of 1

^ Top of page

About Scopus

What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters

Language

日本語に切り替える
切换到简体中文
切換到繁體中文
Русский язык

Customer Service

Help
Contact us