

Kelompok 7

Ararya Pramadani Alief Rahman 215150207111030

Azarya Santoso 215150200111026

Made Diksa Pitra 215150201111025

Judul: AES DHKE File Send & Encryption

Topik: Pengamanan File

1. Carilah topik Anda pada dan temukan judul lain yang mirip dengan judul Anda dan lengkapi dengan tangkapan layar hasilnya :
 - Google Scholar (Total article yang ditemukan : 20, total yang sesuai : 9, total tidak sesuai : 11)

The screenshot displays five search results from Google Scholar. Each result includes a title, authors, publication details, a brief abstract, and interactive links like 'Save', 'Cite', and 'Related articles'. The results are as follows:

- Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing** [PDF] ieee.org
P Rewagad, Y Pawar - 2013 International Conference on ..., 2013 - ieeexplore.ieee.org
... use of digital signature and **Diffie Hellman** key exchange blended with (**AES**) Advanced **Encryption Standard encryption** ... Finally user's data **file** is **encrypted using AES** and only then it is ...
☆ Save Cite Cited by 201 Related articles All 4 versions
- Key management using combination of Diffie-Hellman key exchange with AES encryption** [PDF] ieee.org
Y Yusfiazal, A Meizar, H Kurniawan... - 2018 6th International ..., 2018 - ieeexplore.ieee.org
... the **encrypted file** by using the **Diffie-Hellman** key exchange, after obtaining the ... **file** would be **encrypted** by using **AES** algorithm for **encryption** and decryption **file**, sender would send **file** ...
☆ Save Cite Cited by 21 Related articles
- [PDF] **Data encryption using advanced encryption standard with key generation by elliptic curve diffie-hellman** [PDF] academia.edu
S Sharma, V Chopra - International Journal of Security and Its ..., 2017 - academia.edu
... **AES** and ECDH are used for text **file encryption**. Input text **file** is transformed into **encrypted** form using **AES** algorithm with key generated by ECC and **Diffie-Hellman** will help in ...
☆ Save Cite Cited by 10 Related articles All 2 versions
- File Transfer on Cloud using Diffie-Hellman Key Exchange in Conjunction with AES Encryption** [PDF] ncirl.ie
RB Deokar - 2023 - norma.ncirl.ie
... Now, when an administrator uploads a **file**, the **file** is **encrypted using AES**. The **AES** algorithm employs the SHA256 hashing algorithm. Secure hash algorithm 256-bit (SHA-256) is a ...
☆ Save Cite Related articles All 2 versions
- [PDF] **Cloud computing security improvement using Diffie Hellman and AES** [PDF] psu.edu
R Malik, P Kumar - International Journal of Computer Applications, 2015 - Citeseer
... where data is **encrypted using AES** and Authenticated by **Diffie Hellman** algorithm before it is ... all of the maior business use cases: full disk **encrvotion**. database **encrvotion**. **file** system ...

- IEEE Explore (Total article yang ditemukan : 5, total yang sesuai : 4, total tidak sesuai : 1)

The image displays two screenshots of the IEEE Xplore search results page for the query "file security using DHKE and AES".

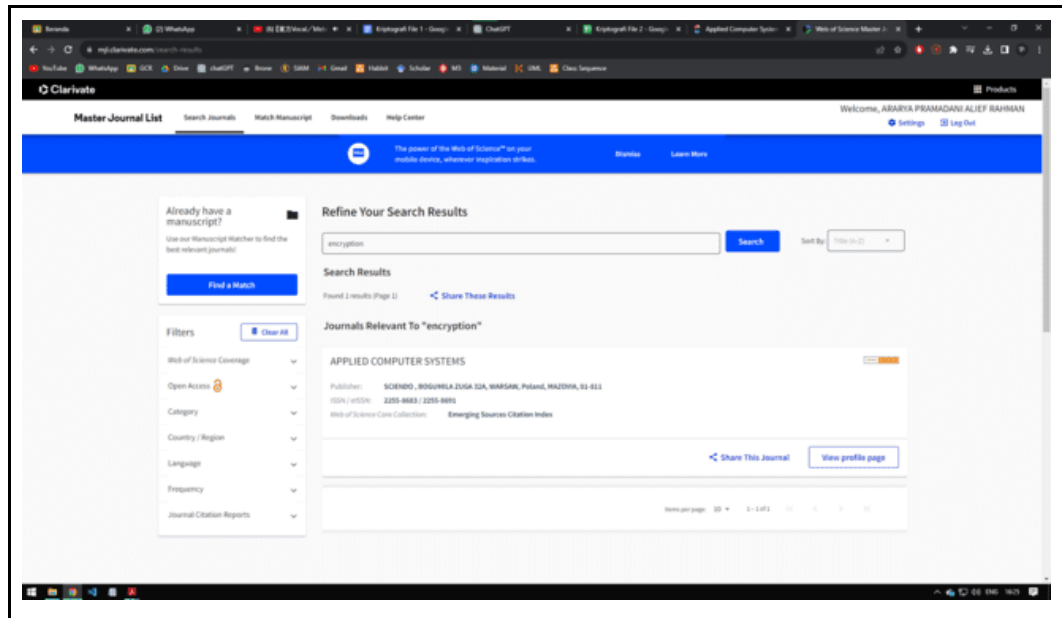
Top Screenshot:

- Search results showing 1-5 of 5 results for "file security using DHKE and AES".
- Filters: All Results (selected), Subscribed Content, Open Access Only.
- Sort By: Relevance.
- Results:
 - A lightweight and secure TFTP protocol for smart environment** by Mohd Anuar Mat Isa; Nur Nabila Mohamed; Habibah Hashim; Syed Farid Syed Adnan; Jamakul-lail Ab Manan; Ramlan Mahmood. 2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE). Year: 2012 | Conference Paper | Publisher: IEEE. Cited by: Papers (16) | Patents (1).
 - Simulation of RSA and ElGamal encryption schemes using RF simulator** by Syed Farid Syed Adnan; Mohd Anuar Mat Isa; Khairul Syazwan Ali Rahman; Mohd Haniff Muhammad; Habibah Hashim. 2015 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE). Year: 2015 | Conference Paper | Publisher: IEEE. Cited by: Papers (1).
 - Securing TFTP packet: A preliminary study** by Nur Nabila Mohamed; Habibah Hashim; Yusnani Mohd Yusoff; Anuar Mat Isa. 2013 IEEE 4th Control and System Graduate Research Colloquium.

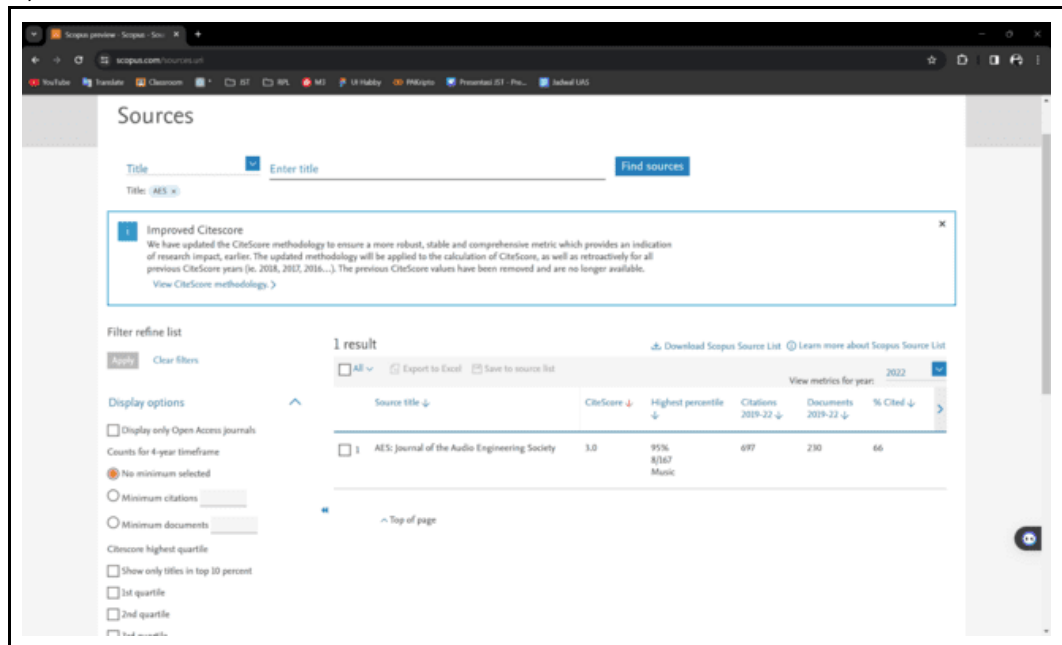
Bottom Screenshot:

- Filters: Author, Affiliation, Publication Title, Publisher, Conference Location, Publication Topics.
- Results:
 - Securing TFTP packet: A preliminary study** by Nur Nabila Mohamed; Habibah Hashim; Yusnani Mohd Yusoff; Anuar Mat Isa. 2013 IEEE 4th Control and System Graduate Research Colloquium. Year: 2013 | Conference Paper | Publisher: IEEE. Cited by: Papers (3).
 - RF simulator for cryptographic protocol** by Mohd Anuar Mat Isa; Habibah Hashim; Jamakul-lail Ab Manan; Syed Farid Syed Adnan; Ramlan Mahmood. 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE 2014). Year: 2014 | Conference Paper | Publisher: IEEE. Cited by: Papers (4).
 - Compression and encryption technique on securing TFTP packet** by Nur Nabila Mohamed; Habibah Hashim; Yusnani Mohd Yusoff; Mohd Anuar Mat Isa; Syed Farid Syed Adnan. 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE). Year: 2014 | Conference Paper | Publisher: IEEE. Cited by: Papers (2).

- ISI Web of Knowledge (Total article yang ditemukan : 1, total yang sesuai : 0, total tidak sesuai : 1)



- Scopus (Total article yang ditemukan : X, total yang sesuai : X, total tidak sesuai : X)



- Elsevier (Total article yang ditemukan : 7, total yang sesuai : 4, total tidak sesuai : 7)

Journal Finder

Find journals | About | Support | My journals | [Register](#) | [Sign in](#)

Showing 1 journal matching your search

Publication type

☒ Journals that offer gold OA

☐ Journals with subscription

CiteScore

All journals

Time to first decision

All journals

Impact factor


All journals

Time to publication

All journals

Cyber Security and Applications

ISSN: 2770-9384



Open Access

Free of charge

Authors do not pay an Article Publishing Charge (APC) in this journal. Your article will be made publicly available in open publication.

View details

Save journal

Visit journal page

Submit paper

Checklist

Impact Factor

Acceptance rate

57%

Time to first decision

5 weeks

Time to publication

4 weeks

ScienceDirect

Journals & Books | [Register](#) | [Sign in](#)

Find articles with these terms

Q85

Journal or book title: Cyber Security and Applications

Advanced search

7 results

sorted by relevance | date

Refine by:

Years

☐ 2024 (2)

☐ 2023 (3)

Article type

☐ Review articles (1)

☐ Research articles (4)

Volumes

☐ 1 (2)

☐ 1 (1)

Subject areas

☐ Computer Science (7)

☐ Mathematics (7)

Access type

☐ Open access & Open archive (7)

Review article • Open access

Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review

Cyber Security and Applications, 10 July 2024

Sudh Ananya Sheik, Anusha Prabakar Murthyend

View PDF

Review article • Open access

Cyber security: State of the art, challenges and future directions

Cyber Security and Applications, 1 October 2023

Wagdy Samir Adnan, Yaghi Hany Mohamed, Alkhatib Alkhatib

View PDF

Would a richer search experience?

Sign in for article preview, additional search fields & filters, and multiple article download & export options.

Sign in

Research article • Open access

Colour image encryption algorithm using Rubik's cube scrambling with bitmap shuffling and frame rotation

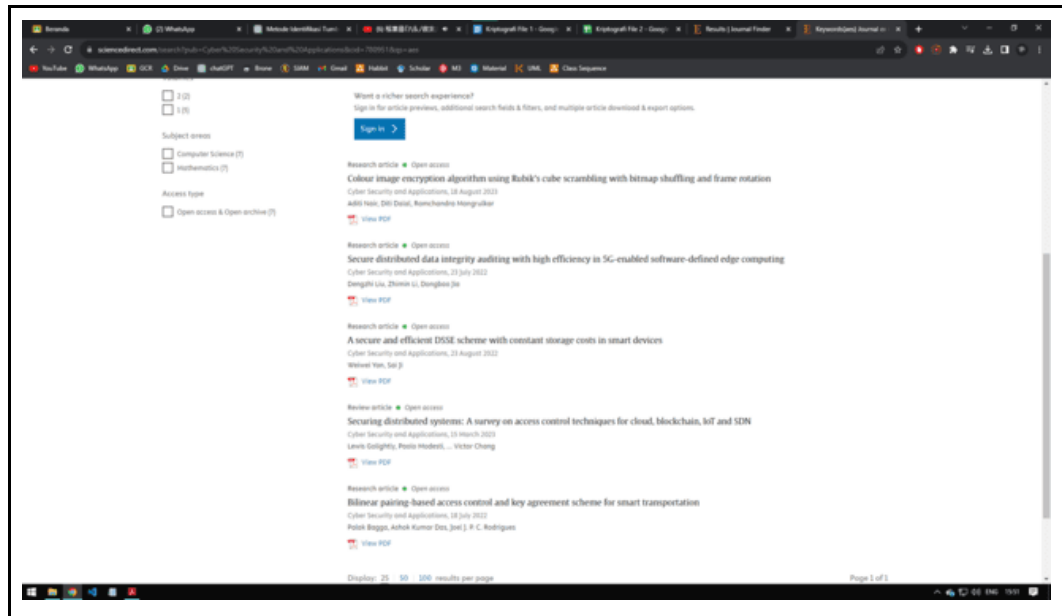
Cyber Security and Applications, 10 August 2023

Aditi Nair, Diti Datta, Rameshchandra Mangulkar

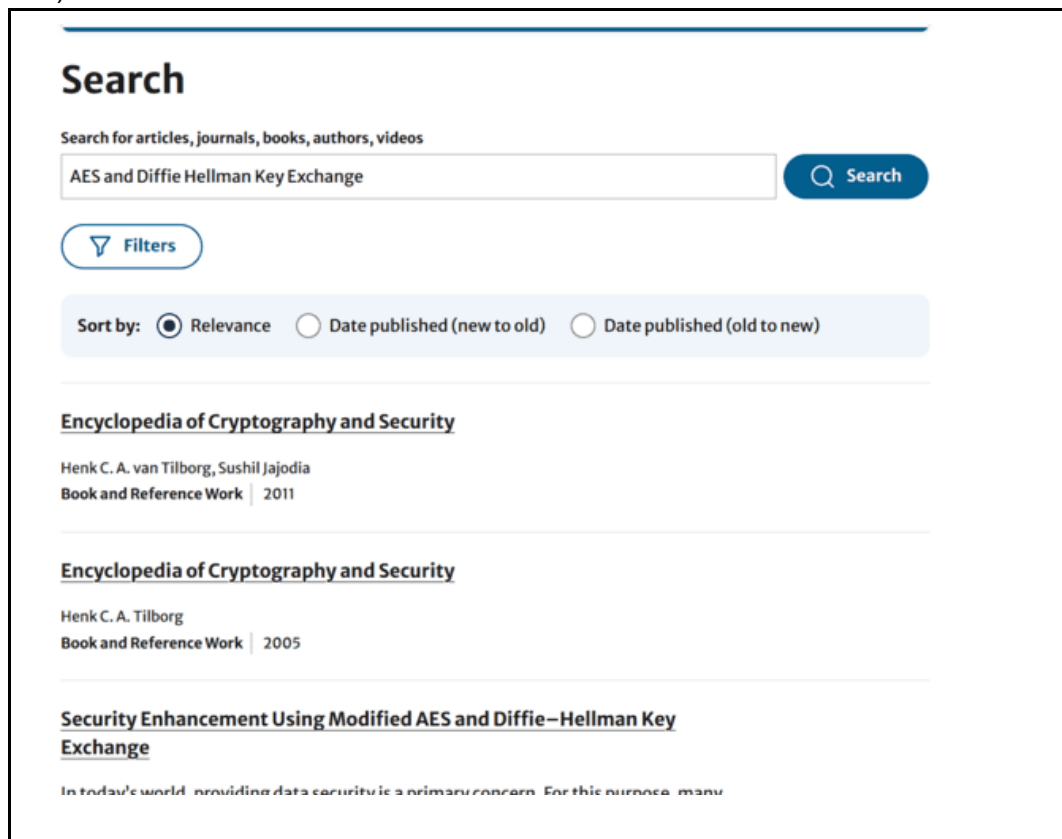
View PDF

Research article • Open access

Secure distributed data integrity auditing with high efficiency in 5G-enabled software-defined edge computing



- Springer (Total article yang ditemukan : 20, total yang sesuai : 0, total tidak sesuai : 20)



2. Keyword apa sajakah yang Anda gunakan? Mengapa Anda menggunakan keyword tersebut?

- File encryption using Aes and Diffie Hellman. Keyword ini merupakan judul dari project akhir kami. Oleh karena itu, kami ingin mengetahui dan mengambil referensi dari jurnal yang sudah ada
- AES and Diffie Hellman Key Exchange. Keyword tersebut merupakan algoritma yang kami pakai di project akhir. Kami menggunakan keyword tersebut agar mendapatkan informasi tambahan mengenai algoritma-algoritma tersebut
- File security using DHKE and AES. Diffie-Hellman (DHKE) dan algoritma enkripsi Advanced Encryption Standard (AES). Keamanan berkas menjadi semakin krusial dalam konteks pengamanan data, dan implementasi DHKE dan AES menawarkan solusi yang efektif untuk melindungi integritas dan kerahasiaan data dalam berkas. DHKE memberikan metode pertukaran kunci yang aman, memungkinkan dua pihak untuk mencapai pertukaran kunci rahasia tanpa perlu mentransmisikan kunci tersebut secara langsung. Sementara itu, AES, sebagai algoritma enkripsi kunci simetris, digunakan untuk mengamankan berkas atau data melalui proses enkripsi dan dekripsi.
- Encryption. Enkripsi adalah proses kunci dalam keamanan berkas. Menekankan kata kunci "encryption" membantu memastikan bahwa penelitian mencakup aspek dasar keamanan yang melibatkan transformasi data menjadi bentuk yang tidak dapat dibaca tanpa memiliki kunci dekripsi yang sesuai.

3. Apa alasan Anda memilih jurnal-jurnal tersebut sebagai kajian pustaka?

Berikut merupakan beberapa alasan kami memilih jurnal-jurnal tersebut sebagai kajian pustaka:

1. Berfokus pada kriptografi dan siber
2. Menyajikan informasi yang terkini dan relevan mengenai implementasi DHKE dan AES dalam konteks pengamanan data
3. Jurnal memberikan informasi penting terhadap judul projek akhir
4. Menggunakan algoritma yang sama yaitu DHKE dan AES
5. Memiliki tujuan yang sama yaitu untuk enkripsi data dan key exchange

4. Apa alasan Anda tidak memilih jurnal-jurnal tersebut sebagai kajian pustaka?

Berikut merupakan beberapa alasan kami tidak memilih jurnal-jurnal tersebut sebagai kajian pustaka:

1. Jurnal sudah lebih dari 5 tahun (dibawah tahun 2018)
2. Memiliki tujuan yang terlalu berbeda jauh
3. Hanya menggunakan salah satu algoritma/ menggunakan algoritma yang berbeda
4. Terdapat duplikasi jurnal
5. Jurnal memberikan informasi yang tidak terlalu penting terhadap judul projek akhir