JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]

# IDENTIFIKASI PERFORMA ALGORITMA BLAKE3 UNTUK VALIDASI DATA

Ariq Muhammad Thabrani [a,1,*], Yusup Miftahuddin [b,2]
[a,b] Institut Teknologi Nasional, Bandung
[1] ariqmuhammadt@mhs.itenas.ac.id*; [2] yusufm@itenas.ac.id;

ARTICLE INFO

**Keywords**
Checksum
Data validation
Hash algorithm

ABSTRACT

This study aims to test the ability and performance of the BLAKE3 algorithm in determining data integrity. The test will conduct a series of trials using the checksum method to obtain the hash value of a data using the BLAKE3 algorithm. The parameters tested are computation time, power consumption, CPU thread, and data size. This test shows that the BLAKE3 algorithm is able to validate data. With this test, the use of the BLAKE3 algorithm has optimal parameters that can be set in order to get the fastest and most efficient results of computing time and power consumption.

## 1. Pendahuluan

Menurut World Bank, hampir 60 persen populasi di dunia menggunakan internet dan Negara Indonesia berada di peringkat ke enam dari 25 Negara yang paling banyak menggunakan internet, masalah yang bisa muncul dengan banyaknya pengguna internet tanpa infrastruktur yang memadai yaitu rusaknya data[1][2]. Salah satu cara untuk mengetahui bahwa suatu data memiliki kerusakan adalah dengan menggunakan metode checksum. Algoritma BLAKE3 termasuk jenis algoritma yang mampu melakukan validasi data. Algoritma BLAKE3 akan melakukan perhitungan hash dari suatu data dengan membagi nya menjadi data berukuran 1 KiloByte dan dilakukan perhitungan checksum di setiap 1 KiloByte tersebut agar bisa menghasilkan nilai hash checksum utama[3]. Algoritma BLAKE3 dapat melakukan validasi data untuk memeriksa apakah data tersebut memiliki kerusakan atau tidak, selain itu algoritma BLAKE3 memiliki kelebihan salah satunya adalah waktu pemrosesannya yang cepat. Penelitian ini menguji kemampuan algoritma BLAKE3 dalam melakukan validasi data, dan juga waktu komputasi dan konsumsi daya yang digunakan saat melakukan pemrosesan data.

Berdasarkan pemaparan tersebut, proses validasi data untuk memastikan data tidak mengalami kerusakan sangat diperlukan, dikarenakan setiap data memiliki informasi yang akan dibaca atau diolah serta pada proses validasi nya diperlukan waktu yang cepat dan konsumsi daya yang efisien[4]. Pada penelitian ini metode algoritma BLAKE3 digunakan sebagai algoritma untuk melakukan validasi data dan menguji waktu komputasi dan konsumsi daya yang digunakan seiring meningkatnya ukuran file dan penggunaan prosesor.

## 2. Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

### 3.1. Spesifikasi Perangkat Keras

Spesifikasi perangkat yang digunakan untuk melakukan pengujian ini yaitu: Prosesor Ryzen 5 3550H (4 core 8 thread), RAM 2x8 GB 3200 Mhz, dan HDD 1 TB.



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

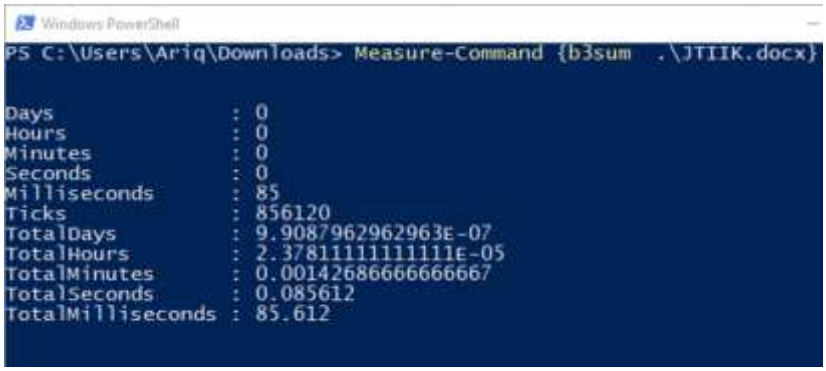
JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]

3.2. Spesifikasi Perangkat Lunak

Pengujian yang dilakukan di penelitian ini menggunakan perangkat lunak dengan informasi berikut: Sistem Operasi Microsoft Windows 10 Versi 21H2, PowerShell versi 5.1.19041.1645, dan b3sum versi 1.3.1.

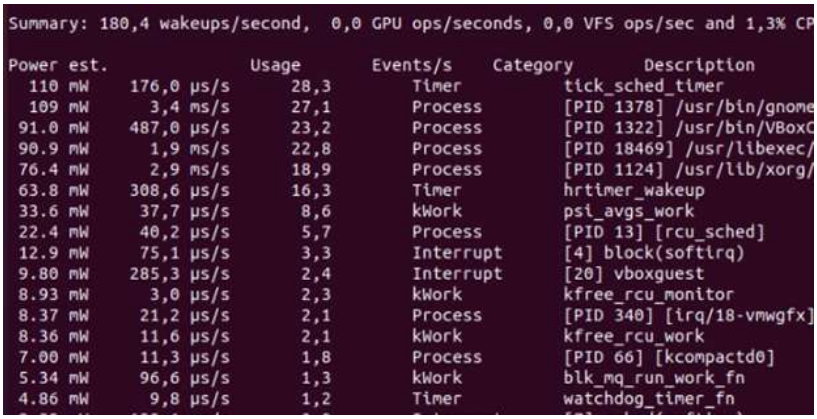
3.3. Perangkat Lunak Pengujian

Perangkat Lunak yang dipakai dalam pengujian ini digunakan untuk mendapatkan data waktu komputasi dan konsumsi daya dari penggunaan algoritma BLAKE3. Perhitungan konsumsi daya menggunakan aplikasi PowerTOP dan perhitungan waktu komputasi menggunakan aplikasi Measure-Command.




Gambar 1. Measure-Command

Di dalam perintah tersebut akan menghitung berapa lama waktu digunakan untuk mengeksekusi suatu perintah. Perintah Measure-Command akan menghasilkan keluaran berupa berapa lama perintah dijalankan mulai dari Hari, Jam, Menit, Detik, dan Milidetik. Waktu yang diambil dari program Measure-Command yaitu milidetik.




Gambar 2. PowerTOP

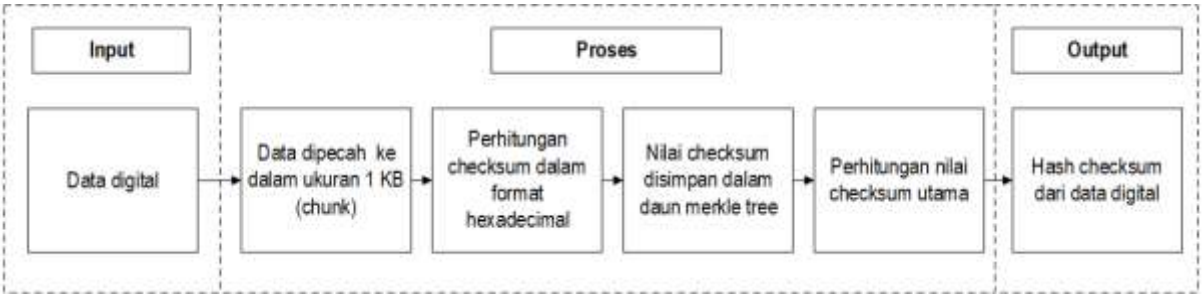
Proses perhitungan konsumsi daya menggunakan program.PowerTOP yang akan menampilkan estimasi penggunaan daya dari suatu program. PowerTOP merupakan suatu perangkat lunak tambahan yang digunakan dalam pengujian ini untuk melihat konsumsi daya yang digunakan oleh algoritma BLAKE3 saat perhitungan nilai checksum.



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]

Dalam memahami pengujian di dalam penelitian ini diperlukan alur tahapan pengujian, salah satu caranya adalah dengan membuat blok diagram. Berikut ini adalah model blok diagram input-proses-output yang digambarkan pada Gambar 3.




Gambar 3. Blok Diagram Pengujian

a. Input berupa data digital dalam bentuk atau format apapun misalnya DOCX, PDF, JPG, dan sebagainya yang akan diproses oleh algoritma BLAKE3 menggunakan B3sum.
b. Proses terdiri dari proses pemecahan data menjadi 1KB chunk yang kemudian akan dilakukan proses perhitungan nilai checksum oleh algoritma BLAKE3. Setiap nilai checksum dari keseluruhan potongan data kemudian akan dihitung ulang menggunakan metode Merkle Tree sehingga mendapatkan nilai checksum utama.
c. Output akan mengeluarkan nilai hash berupa nilai checksum utama yang bisa digunakan untuk memvalidasi atau memverifikasi keutuhan suatu data digital.

## 2. Hasil dan Pembahasan

Pengujian dalam penelitian ini menggunakan data digital yang dibuat dengan command line interface untuk membuat data sembarang yang berukuran 1 Megabyte, 10 Megabyte, 100 Megabyte, dan 1 Gigabyte.

### 3.1. Hasil Pengujian File Berukuran 1 MB

Tabel 1. Hasil Pengujian File 1 Megabyte

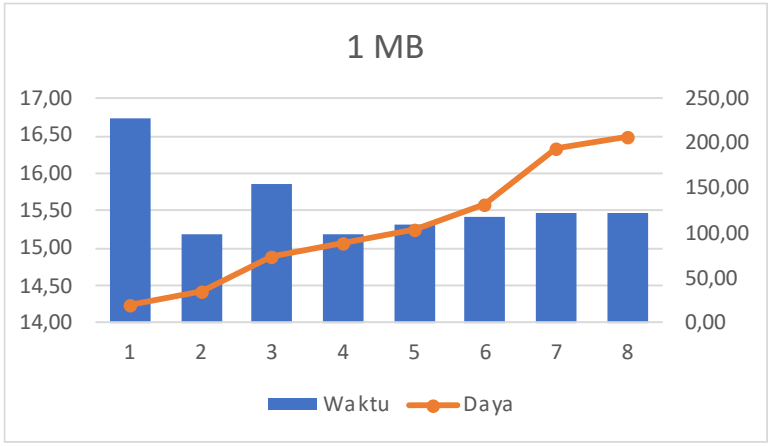
| Thread | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| **Waktu (ms)** | 16,75 | 15,18 | 15,87 | 15,18 | 15,31 | 15,41 | 15,47 | 15,47 |
| **Waktu %** | 100% | 9,4% | 5,3% | 9,4% | 8,6% | 8,0% | 7,7% | 7,7% |
| **Daya (mW)** | 20,10 | 35,34 | 73,50 | 89,86 | 105,13 | 133,36 | 194,99 | 208,36 |
| **Daya %** | 100% | 176% | 366% | 447% | 523% | 663% | 970% | 1037% |

Pada pengujian file berukuran 1 MB dengan 1 thread memakan waktu selama 16,75 ms dengan konsumsi daya 20,1 mW, dan dengan 8 thread hanya mendapatkan peningkatan waktu komputasi hampir 8% menjadi 15,47 ms tapi dengan konsumsi daya lebih banyak yakni lebih dari 10x lipat di 208,36 mW.



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]



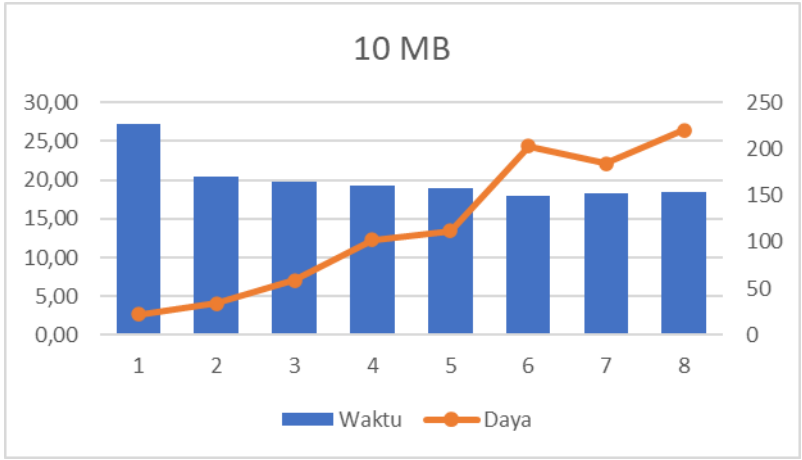

Gambar 4. Hasil Pengujian File 1 Megabyte

3.2. Hasil Pengujian File Berukuran 10 MB

Tabel 2. Hasil Pengujian File 10 Megabyte

| Thread | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| **Waktu (ms)** | 27,19 | 20,37 | 19,80 | 19,33 | 18,95 | 17,95 | 18,34 | 18,45 |
| **Waktu %** | 100% | 25,1% | 27,2% | 28,9% | 30,3% | 34,0% | 32,6% | 32,2% |
| **Daya (mW)** | 22,10 | 34,15 | 59,00 | 102,06 | 112,06 | 203,40 | 184,40 | 220,31 |
| **Daya %** | 100% | 160% | 333% | 407% | 476% | 603% | 882% | 943% |

Pada pengujian file berukuran 10 MB dengan 1 thread memakan waktu selama 27,19 ms dengan konsumsi daya 22,1 mW, dan dengan 8 thread didapat peningkatan waktu komputasi sebanyak 32% menjadi 18,45 ms tapi dengan konsumsi daya lebih banyak yakni lebih dari 9 kali lipat di 220,31 mW.




Gambar 5. Hasil Pengujian File 10 Megabyte



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

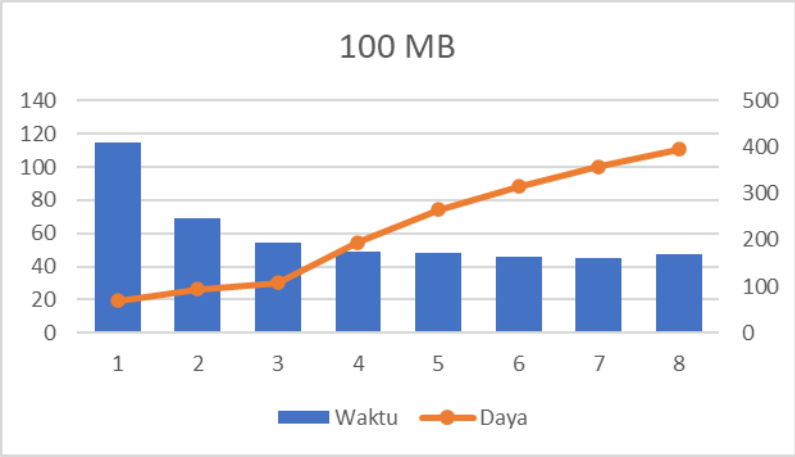
JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]

3.3. Hasil Pengujian File Berukuran 100 MB

Tabel 3. Hasil Pengujian File 100 Megabyte

| Thread | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Waktu (ms) | 114,59 | 68,80 | 54,70 | 48,87 | 47,92 | 46,12 | 45,40 | 47,16 |
| Waktu % | 100% | 40,0% | 52,3% | 57,3% | 58,2% | 59,8% | 60,4% | 58,8% |
| Daya (mW) | 69,00 | 93,40 | 107,30 | 194,80 | 264,70 | 314,60 | 357,80 | 394,90 |
| Daya % | 100% | 135% | 156% | 282% | 384% | 456% | 519% | 572% |

Pada pengujian file berukuran 100 MB dengan 1 thread memakan waktu selama 114,59 ms dengan konsumsi daya 69 mW, dan dengan 8 thread didapat peningkatan waktu komputasi sebesar 58,8% menjadi 47,16 ms tapi dengan konsumsi daya lebih banyak yakni lebih dari 5 kali lipat di 394,9 mW.




Gambar 6. Hasil Pengujian File 100 Megabyte

3.4. Hasil Pengujian File Berukuran 1 GB

Tabel 4. Hasil Pengujian File 1 Gigabyte

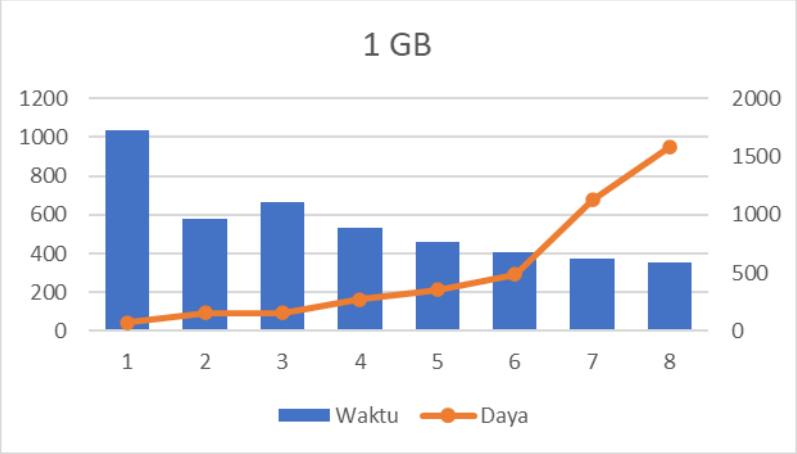
| Thread | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Waktu (ms) | 1037,68 | 577,07 | 663,71 | 531,62 | 458,02 | 406,50 | 372,57 | 355,79 |
| Waktu % | 100% | 44,4% | 36,0% | 48,8% | 55,9% | 60,8% | 64,1% | 65,7% |
| Daya (mW) | 74,90 | 156,30 | 156,40 | 269,10 | 353,70 | 488,20 | 1125,00 | 1585,00 |
| Daya % | 100% | 209% | 209% | 359% | 472% | 652% | 1502% | 2116% |

Pada pengujian file berukuran 1 GB dengan 1 thread memakan waktu selama 1037,68 ms dengan konsumsi daya 74,9 mW, dan dengan 8 thread mendapatkan peningkatan waktu komputasi sebanyak 65,7% menjadi 355,79 ms tapi dengan konsumsi daya lebih banyak yakni lebih dari 21 kali lipat di 1585 mW.



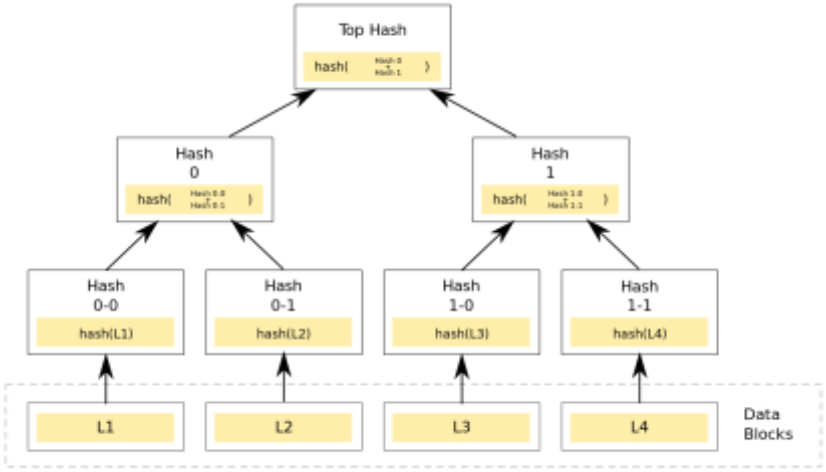
https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]




Gambar 7. Hasil Pengujian File 1 Gigabyte

Hasil akhir menunjukkan bahwa konsumsi daya akan meningkat seiring dengan waktu komputasi yang semakin cepat dengan banyaknya jumlah thread CPU yang digunakan tetapi ada titik dimana waktu komputasi akan mencapai tingkat efisiensi terbaik tergantung dengan ukuran file yang diuji dan jumlah CPU thread yang digunakan.




Gambar 8. Merkle Tree

Semakin besar file yang diuji maka waktu komputasi akan semakin meningkat yang membuat semakin banyaknya blok data. Hal ini dikarenakan algoritma BLAKE3 menggunakan metode Merkle Tree yang memecah data ke dalam ukuran 1 Kilobyte blok data untuk kemudian dilakukan perhitungan hash dari blok data tersebut. Setiap hash dari satu blok data akan dikombinasikan dengan blok data selanjutnya yang akan menghasilkan nilai hash baru secara terus menerus hingga menghasilkan hash utama (*root hash/top hash).*



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 17 No 1]
[Januari 2023]

3.5. Penggunaan Random Access Memory (RAM) dalam KiloByte (KB)

Tabel 5. Penggunaan Memori (RAM)

| Thread | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| **1 MB** | 275 | 339 | 316 | 333 | 323 | 409 | 325 | 412 |
| **10 MB** | 459 | 400 | 378 | 483 | 446 | 589 | 558 | 632 |
| **100 MB** | 611 | 622 | 709 | 746 | 800 | 820 | 880 | 954 |
| **1 GB** | 636 | 679 | 725 | 773 | 826 | 877 | 932 | 960 |

Penggunaan memori (RAM) saat pengujian menunjukkan peningkatan konsumsi memori seiring dengan banyaknya jumlah thread CPU yang digunakan, peningkatan terlihat lebih signifikan di pengujian file yang berukuran besar.


Gambar 9. Penggunaan Random Access Memory (RAM)

## 3. Kesimpulan

Berdasarkan hasil pengujian, ditarik kesimpulan bahwa Algoritma BLAKE3 sanggup untuk melakukan validasi data digital dengan cepat dan efisien dikarenakan menggunakan metode Merkle Tree. Agar mencapai hasil yang paling efisien, untuk file berukuran 1 MB cukup menggunakan 1 thread CPU, 10 MB menggunakan 2 thread CPU, 100 MB menggunakan 3 thread CPU, dan 1 GB menggunakan 4 hingga 6 thread CPU. Ukuran file dan jumlah thread CPU mempengaruhi waktu komputasi dan konsumsi daya yang digunakan oleh algoritma BLAKE3.

## Daftar Pustaka

[1] S. Setti and A. Wanto, "Analysis of Backpropagation Algorithm in Predicting the Most Number of Internet Users in the World," Jurnal Online Informatika, vol. 3, no. 2, pp. 110–115, 2018, doi: 10.15575/join.

[2] R. I. Ciobanu, V. C. Tăbuşcă, C. Dobre, L. Băjenaru, C. X. Mavromoustakis, and G. Mastorakis, "Avoiding Data Corruption in Drop Computing Mobile Networks," IEEE Access, vol. 7, pp. 31170–31185, 2019, doi: 10.1109/ACCESS.2019.2903018.



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI

[3] J. O'Connor, J.-P. Aumasson, S. Neves, and Z. Wilcox-O'Hearn, "BLAKE3 one function, fast everywhere." [Online]. Available: https://blake3.io

[4] A. S. G. Andrae, "Hypotheses for primary energy use, electricity use and CO2 emissions of global computing and its shares of the total between 2020 and 2030," WSEAS Transactions on Power Systems, vol. 15, pp. 50–59, Mar. 2020, doi: 10.37394/232016.2020.15.6.

[5] A. M. Qadir and N. Varol, "A review paper on cryptography," 7th International Symposium on Digital Forensics and Security, ISDFS 2019, Jun. 2019, doi: 10.1109/ISDFS.2019.8757514.

[6] H. Roy, D. B.-I. J. of M. L. and, and undefined 2017, "Face sketch-photo recognition using local gradient checksum: LGCS," Springer, vol. 8, no. 5, pp. 1457–1469, Oct. 2017, doi: 10.1007/s13042-016-0516-0.

[7] Y. bin Idris, S. Adli Ismail, N. F. Mohd Azmi, A. Azmi, and A. Azizan, "Enhancement Data Integrity Checking Using Combination MD5 and SHA1 Algorithm in Hadoop Architecture," Journal of Computer Science & Computational Mathematics, pp. 99–102, Sep. 2017, doi: 10.20967/jcscm.2017.03.007.

[8] N. Katrandzhiev, D. Hristozov, and B. Milenkov, "A COMPARISON OF PASSWORD PROTECTION METHODS FOR WEB-BASED PLATFORMS IMPLEMENTED WITH PHP AND MYSQL."

[9] Kahri Fatma, Bouallegue Belgacem, Machhout Mohsen, and Tourki Rached, An FPGA Implementation and Comparison of the SHA-256 and Blake-256.

[10] Mota Aquino Valentim, Azam Sami, Shanmugam Bharanidharan, Yeo Kheng Cher, and Kannoorpatti Krishnan, "Comparative Analysis of Different Techniques of Encryption for Secured Data Transmission," IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 231–237, 2017, doi: 10.1109/ICPCSI.2017.8392158.

[11] S. Long, "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512," in Journal of Physics: Conference Series, Nov. 2019, vol. 1314, no. 1. doi: 10.1088/1742-6596/1314/1/012210.

[12] Y.-H. Xia, H.-S. Hong, G.-F. Lin, and Z.-X. Sun, "Efficient Data Integrity Verification Using CRC Based on HDFS in Cloud Storage."

[13] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," in Journal of Physics: Conference Series, Mar. 2018, vol. 978, no. 1. doi: 10.1088/1742-6596/978/1/012116.

[14] S. Sinha, S. Anand, and K. Prakasha, "Improving Smart Contract Transaction Performance in Hyperledger Fabric; Improving Smart Contract Transaction Performance in Hyperledger Fabric," 2021, doi: 10.1109/ETI4.051663.2021.9619202.

[15] I. Teodora Ciocan, E. Alexandra Kelesidis, D. Maimut, and L. Morogan, "A Modified Argon2i Using a Tweaked Variant of Blake3," 2021 26th IEEE Asia-Pacific Conference on Communications (APCC), 2021, doi: 10.1109/APCC49754.2021.9609933.



https://doi.org/10.47111/JTI
Available online at https://e-journal.upr.ac.id/index.php/JTI