IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

Analisis Komparatif Kinerja Komputasi Brute Force pada Arsitektur GPU NVIDIA Turing, Ampere, dan Ada Lovelace

Miko Kastomo Putro

Program Studi Teknik Komputer
Fakultas Ilmu Komputer
Universitas Amikom Yogyakarta, Jl Padjajaran, Ring Road Utara, Yogyakarta 55281, Indonesia

Author Emails
[a)] Corresponding author: miko.putro@amikom.ac.id

Abstract. *In digital forensic investigations, the effectiveness of brute force attacks for password recovery relies heavily on hardware computational capacity. This study aims to evaluate and compare the performance of three generations of NVIDIA mid-range Graphics Processing Units (GPUs): GeForce GTX 1660 Ti (Turing), RTX 3050 (Ampere), and RTX 4060 (Ada Lovelace). The research employs a quantitative experimental method using Hashcat software to measure hashrate, latency, and temperature across three algorithms with varying complexities: MD5, SHA-256, and Bcrypt. The results demonstrate that the RTX 4060 dominates all test scenarios with significant performance improvements. However, an anomalous phenomenon was observed in the comparison of previous generations. In memory-bound algorithms (MD5 and SHA-256), the GTX 1660 Ti outperformed the RTX 3050 by up to 47% due to its superior 192-bit memory bus width. Conversely, in compute-bound algorithms (Bcrypt), the RTX 3050 surpassed the GTX 1660 Ti by twofold, attributed to the efficiency of its modern core architecture. This study concludes that while the latest architecture (RTX 4060) offers the best performance, hardware selection on a limited budget must be tailored to the target algorithm characteristics, where memory bus specifications are a crucial factor for lightweight algorithms.*

***Keywords*:**
Brute Force, Digital Forensics, GPU, Hashcat, Computational Performance

Abstraksi. Dalam investigasi forensik digital, efektivitas serangan brute force untuk pemulihan kata sandi sangat bergantung pada kapasitas komputasi perangkat keras. Penelitian ini bertujuan untuk mengevaluasi dan membandingkan kinerja tiga generasi Graphics Processing Unit (GPU) kelas menengah NVIDIA, yaitu GeForce GTX 1660 Ti (Turing), RTX 3050 (Ampere), dan RTX 4060 (Ada Lovelace). Metode penelitian menggunakan pendekatan eksperimental kuantitatif dengan perangkat lunak Hashcat untuk mengukur hashrate, latensi, dan suhu pada tiga algoritma dengan kompleksitas berbeda: MD5, SHA-256, dan Bcrypt. Hasil pengujian menunjukkan bahwa RTX 4060 mendominasi seluruh skenario pengujian dengan peningkatan kinerja signifikan. Namun, ditemukan fenomena anomali pada komparasi generasi sebelumnya. Pada algoritma berbasis memory-bound (MD5 dan SHA-256), GTX 1660 Ti justru mengungguli RTX 3050 hingga 47% karena keunggulan lebar jalur memori 192-bit. Sebaliknya, pada algoritma compute-bound (Bcrypt), RTX 3050 berbalik unggul dua kali lipat dibandingkan GTX 1660 Ti berkat efisiensi arsitektur core yang lebih modern. Penelitian ini menyimpulkan bahwa meskipun arsitektur terbaru (RTX 4060) menawarkan performa terbaik, pemilihan perangkat keras pada anggaran terbatas harus disesuaikan dengan karakteristik target algoritma, di mana spesifikasi memory bus menjadi faktor krusial untuk algoritma ringan..

Kata Kunci:
Brute Force, Forensik Digital, GPU, Hashcat, Kinerja Komputasi

IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

PENDAHULUAN

Dalam ekosistem keamanan siber kontemporer, integritas data dan kekuatan autentikasi merupakan pertahanan garis depan melawan akses ilegal. Salah satu vektor ancaman yang paling persisten dan mendasar adalah serangan brute force, sebuah metode deterministik yang mengeksploitasi kelemahan manajemen kata sandi melalui pencarian menyeluruh. Efektivitas serangan ini sangat bergantung pada kapasitas komputasi perangkat keras yang digunakan. Dekade terakhir telah menyaksikan pergeseran paradigma komputasi forensik dari pemrosesan berbasis Central Processing Unit (CPU) menuju General-Purpose Computing on Graphics Processing Units (GPGPU). Arsitektur paralel masif pada GPU memungkinkan eksekusi ribuan instruksi hashing secara simultan, memberikan keunggulan kecepatan yang signifikan dibandingkan arsitektur serial tradisional. Evolusi teknologi ini tercermin jelas pada inovasi arsitektur NVIDIA, mulai dari Turing yang memperkenalkan efisiensi instruksi konkuren, Ampere dengan peningkatan throughput data, hingga Ada Lovelace yang menawarkan litografi 4nm dengan fokus pada efisiensi daya.

Sejumlah penelitian terdahulu telah mendokumentasikan lonjakan kinerja komputasi ini. Vastrad dan Naik membuktikan bahwa dalam skenario pemecahan sandi, GPU mampu memberikan akselerasi hingga 50 kali lipat dibandingkan CPU kelas atas [1]. Temuan ini diperkuat oleh Choquette dkk., yang mencatat bahwa arsitektur Ampere mampu menggandakan kinerja komputasi mentah dibandingkan generasi sebelumnya melalui peningkatan CUDA Cores [4]. Namun, Brothers dkk. menyoroti bahwa kendala utama pada implementasi arsitektur modern adalah konsumsi daya yang tinggi saat beroperasi pada beban penuh, yang berimplikasi langsung pada efisiensi biaya operasional [5]. Di sisi lain, analisis teknis oleh Wong mengenai arsitektur Ada Lovelace menunjukkan potensi efisiensi tinggi berkat peningkatan L2 Cache yang signifikan [6]. Meskipun demikian, literatur yang ada saat ini masih parsial dan jarang membandingkan kinerja ketiga generasi tersebut secara spesifik pada segmen kartu grafis kelas menengah (mid-range), yang notabene merupakan perangkat paling terjangkau dan banyak digunakan oleh praktisi keamanan siber maupun peneliti independen.

Merespons dinamika tersebut, penelitian ini bertujuan untuk melakukan analisis komparatif kinerja komputasi brute force pada tiga generasi arsitektur NVIDIA yang diwakili oleh varian kelas menengah. Sampel penelitian difokuskan pada GeForce GTX 1660 Ti sebagai representasi arsitektur Turing, GeForce RTX 3050 varian 6GB sebagai representasi arsitektur Ampere, dan GeForce RTX 4060 varian 8GB sebagai representasi arsitektur Ada Lovelace. Pemilihan varian ini didasarkan pada posisi pasar mereka sebagai penerus di kelas yang setara, sehingga memungkinkan perbandingan yang adil (apple-to-apple) terkait evolusi kinerja. Metodologi penelitian menerapkan pendekatan eksperimental kuantitatif menggunakan perangkat lunak Hashcat sebagai standar industri untuk melakukan benchmarking terhadap tiga algoritma dengan tingkat kompleksitas berbeda, yaitu MD5, SHA-256, dan Bcrypt.

Penelitian ini dibatasi pada analisis parameter teknis yang meliputi kecepatan pemecahan (hashrate), suhu operasional maksimal, dan konsumsi daya listrik, serta tidak membahas aspek pengembangan algoritma kriptografi baru. Kontribusi utama dari makalah ini adalah menyediakan data empiris yang komprehensif mengenai karakteristik penskalaan kinerja antar generasi pada perangkat keras mainstream. Hasil analisis diharapkan dapat memberikan wawasan strategis mengenai arsitektur mana yang menawarkan rasio performa terhadap daya (performance-per-watt) dan performa terhadap harga (price-to-performance) terbaik. Temuan ini ditujukan menjadi rujukan valid bagi investigator forensik digital dan auditor keamanan sistem dalam menentukan spesifikasi perangkat keras yang paling efisien untuk mendukung operasional pengujian penetrasi.

TINJAUAN PUSTAKA

Transformasi metode pengujian penetrasi keamanan saat ini didominasi oleh pemanfaatan General-Purpose Computing on Graphics Processing Units (GPGPU). Sanders dan Kandrot menjelaskan bahwa arsitektur dasar GPU yang terdiri dari ribuan core pemrosesan kecil memungkinkan eksekusi paralel yang masif, sebuah karakteristik yang sangat ideal untuk algoritma kriptografi bersifat data-parallel [8]. Dalam konteks serangan brute force, efisiensi perangkat keras diukur berdasarkan throughput atau jumlah hash yang dapat dihitung per detik. Manavski menegaskan bahwa kinerja ini sangat bergantung pada kemampuan arsitektur memori dan Arithmetic Logic Unit (ALU) dalam menangani instruksi tanpa mengalami kemacetan (bottleneck) [9]. Oleh karena itu, pemahaman mendalam mengenai

IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

karakteristik mikroarsitektur pada setiap generasi GPU menjadi fundamental dalam analisis kinerja komputasi forensik.

Penelitian ini membedah evolusi teknologi NVIDIA melalui tiga sampel representatif di kelas menengah. Arsitektur Turing, yang diwakili oleh GTX 1660 Ti, memperkenalkan eksekusi konkuren untuk operasi Integer dan Floating Point. Jia dkk. mencatat bahwa meskipun varian GTX tidak memiliki Tensor Cores seperti seri RTX, fitur eksekusi konkuren ini tetap memberikan efisiensi instruksi yang signifikan dibandingkan generasi Pascal sebelumnya [2]. Evolusi berlanjut pada arsitektur Ampere yang diwakili oleh RTX 3050 6GB, yang membawa peningkatan pada jalur data FP32. Choquette dkk. memaparkan bahwa Ampere dirancang untuk menggandakan kinerja komputasi per siklus jam [4], namun pada varian entry-level seperti RTX 3050, kinerja ini seringkali dibatasi oleh lebar jalur memori (memory bus) yang lebih sempit. Generasi terbaru, Ada Lovelace pada RTX 4060 8GB, mengatasi batasan tersebut melalui peningkatan drastis pada L2 Cache. Wong menyoroti bahwa L2 Cache yang besar berfungsi mengurangi latensi akses ke VRAM, sehingga menjaga stabilitas kinerja pada beban kerja intensif [6].

Tinjauan terhadap literatur terdahulu menunjukkan beberapa temuan penting terkait akselerasi perangkat keras. Vastrad dan Naik telah memvalidasi superioritas GPU terhadap CPU dengan akselerasi hingga 50 kali lipat pada algoritma MD5 [1]. Namun, penelitian tersebut menggunakan perangkat keras yang kini telah usang. Brothers dkk. memperbarui diskursus ini dengan mengevaluasi arsitektur Ampere pada lingkungan cloud dan mencatat peningkatan kinerja yang substansial, namun juga menggarisbawahi isu tingginya konsumsi daya yang berbanding lurus dengan biaya operasional [5]. Hal ini sejalan dengan peringatan Martínez dkk. bahwa efisiensi energi atau performance-per-watt seringkali menurun drastis ketika GPU dipaksa bekerja pada frekuensi maksimum dalam durasi lama [3].

Meskipun penelitian mengenai kinerja GPU cukup ekstensif, terdapat kesenjangan literatur yang nyata pada segmen perangkat keras kelas menengah (mid-range). Sebagian besar studi, termasuk laporan teknis NVIDIA [7], cenderung berfokus pada kartu grafis kelas atas (flagship) atau kinerja gaming, sehingga kurang relevan bagi praktisi forensik dengan anggaran terbatas. Belum terdapat studi komparatif yang secara spesifik membedah kinerja GTX 1660 Ti, RTX 3050, dan RTX 4060 dalam satu skenario pengujian hashing yang terkontrol. Ketiadaan data ini menyulitkan pengambilan keputusan terkait efektivitas biaya saat melakukan peremajaan perangkat keras. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan menyajikan analisis komprehensif mengenai rasio performa terhadap harga dan daya pada ketiga generasi arsitektur tersebut, memberikan landasan empiris bagi pemilihan infrastruktur keamanan siber yang efisien.

METODE PENELITIAN

Transformasi metode pengujian penetrasi keamanan saat ini didominasi oleh pemanfaatan General-Purpose Computing on Graphics Processing Units (GPGPU). Sanders dan Kandrot menjelaskan bahwa arsitektur dasar GPU yang terdiri dari ribuan core pemrosesan kecil memungkinkan eksekusi paralel yang masif, sebuah karakteristik yang sangat ideal untuk algoritma kriptografi bersifat data-parallel [8]. Dalam konteks serangan brute force, efisiensi perangkat keras diukur berdasarkan throughput atau jumlah hash yang dapat dihitung per detik. Manavski menegaskan bahwa kinerja ini sangat bergantung pada kemampuan arsitektur memori dan Arithmetic Logic Unit (ALU) dalam menangani instruksi tanpa mengalami kemacetan (bottleneck) [9]. Oleh karena itu, pemahaman mendalam mengenai karakteristik mikroarsitektur pada setiap generasi GPU menjadi fundamental dalam analisis kinerja komputasi forensik.

Penelitian ini membedah evolusi teknologi NVIDIA melalui tiga sampel representatif di kelas menengah. Arsitektur Turing, yang diwakili oleh GTX 1660 Ti, memperkenalkan eksekusi konkuren untuk operasi Integer dan Floating Point. Jia dkk. mencatat bahwa meskipun varian GTX tidak memiliki Tensor Cores seperti seri RTX, fitur eksekusi konkuren ini tetap memberikan efisiensi instruksi yang signifikan dibandingkan generasi Pascal sebelumnya [2]. Evolusi berlanjut pada arsitektur Ampere yang diwakili oleh RTX 3050 6GB, yang membawa peningkatan pada jalur data FP32. Choquette dkk. memaparkan bahwa Ampere dirancang untuk menggandakan kinerja komputasi per siklus jam [4], namun pada varian entry-level seperti RTX 3050, kinerja ini seringkali dibatasi oleh lebar jalur memori (memory bus) yang lebih sempit. Generasi terbaru, Ada Lovelace pada RTX 4060 8GB, mengatasi batasan tersebut

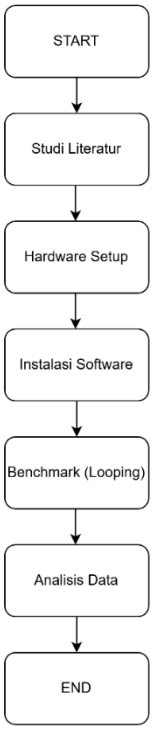
IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

melalui peningkatan drastis pada L2 Cache. Wong menyoroti bahwa L2 Cache yang besar berfungsi mengurangi latensi akses ke VRAM, sehingga menjaga stabilitas kinerja pada beban kerja intensif [6].

Tinjauan terhadap literatur terdahulu menunjukkan beberapa temuan penting terkait akselerasi perangkat keras. Vastrad dan Naik telah memvalidasi superioritas GPU terhadap CPU dengan akselerasi hingga 50 kali lipat pada algoritma MD5 [1]. Namun, penelitian tersebut menggunakan perangkat keras yang kini telah usang. Brothers dkk. memperbarui diskursus ini dengan mengevaluasi arsitektur Ampere pada lingkungan cloud dan mencatat peningkatan kinerja yang substansial, namun juga menggarisbawahi isu tingginya konsumsi daya yang berbanding lurus dengan biaya operasional [5]. Hal ini sejalan dengan peringatan Martínez dkk. bahwa efisiensi energi atau performance-per-watt seringkali menurun drastis ketika GPU dipaksa bekerja pada frekuensi maksimum dalam durasi lama [3].

Meskipun penelitian mengenai kinerja GPU cukup ekstensif, terdapat kesenjangan literatur yang nyata pada segmen perangkat keras kelas menengah (mid-range). Sebagian besar studi, termasuk laporan teknis NVIDIA [7], cenderung berfokus pada kartu grafis kelas atas (flagship) atau kinerja gaming, sehingga kurang relevan bagi praktisi forensik dengan anggaran terbatas. Belum terdapat studi komparatif yang secara spesifik membedah kinerja GTX 1660 Ti, RTX 3050, dan RTX 4060 dalam satu skenario pengujian hashing yang terkontrol. Ketiadaan data ini menyulitkan pengambilan keputusan terkait efektivitas biaya saat melakukan peremajaan perangkat keras. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan menyajikan analisis komprehensif mengenai rasio performa terhadap harga dan daya pada ketiga generasi arsitektur tersebut, memberikan landasan empiris bagi pemilihan infrastruktur keamanan siber yang efisien.

Bagian ini memuat penjelasan secara lengkap dan terinci tentang langkah-langkah yang dilakukan dalam melakukan penelitian ini. Selain itu, langkah penelitian juga perlu ditunjukkan dalam bentuk diagram alir langkah penelitian atau framework secara lengkap dan terinci termasuk di dalamnya tercermin algoritma, rule, pemodelan-pemodelan, desain dan lain-lain yang terkait dengan aspek perancangan sistem.



GAMBAR 1. Alur Penelitian

IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

HASIL DAN PEMBAHASAN

Analisis Kinerja Komputasi Pada Algoritma MD5

TABEL 1. Hasil Kinerja Komputasi Algoritma MD5

MD5	Hashrate	Latency (ms)	Suhu Max (°C)
GTX 1660TI 6GB	20774.08 MH/s	76.922	52.48
RTX 3050 6GB	14121.32 MH/s	84.856	46.8
RTX 4060 8GB	29892.3 MH/s	53.47	62.82

Analisis kinerja komputasi pada algoritma MD5 memperlihatkan dominasi mutlak arsitektur Ada Lovelace, di mana GeForce RTX 4060 8GB mencatatkan throughput tertinggi sebesar 29.892,3 MH/s dengan latensi terendah 53,47 ms, menegaskan efektivitas arsitektur terbaru dalam menangani instruksi hashing masif. Namun, temuan yang cukup kontraintuitif teramati pada komparasi antar-generasi sebelumnya, di mana GeForce GTX 1660 Ti (Turing) secara mengejutkan mengungguli GeForce RTX 3050 6GB (Ampere). GTX 1660 Ti mampu mencapai kecepatan 20.774,08 MH/s dengan suhu stabil di 52,48°C, sedangkan RTX 3050 tertinggal signifikan di angka 14.121,32 MH/s dengan latensi terburuk mencapai 84,856 ms. Disparitas kinerja ini mengindikasikan bahwa pemangkasan lebar jalur memori pada RTX 3050 menjadi hambatan krusial (bottleneck) bagi algoritma MD5 yang sangat bergantung pada bandwidth, sehingga arsitektur core yang lebih modern tidak dapat bekerja maksimal. Hal ini turut tercermin pada suhu RTX 3050 yang sangat rendah di 46,8°C, yang bukan menandakan efisiensi pendinginan semata, melainkan gejala underutilization akibat kemacetan aliran data, berbeda dengan RTX 4060 yang mencapai suhu 62,82°C sebagai konsekuensi logis dari tingginya beban pemrosesan yang berhasil dieksekusi.

Analisis Kinerja Komputasi Pada Algoritma SHA-256

TABEL 2. Hasil Kinerja Komputasi Algoritma SHA-256

SHA-256	Hashrate	Latency (ms)	Suhu Max (°C)
GTX 1660TI 6GB	2914.2 MH/s	68.712	51.86
RTX 3050 6GB	2007.22 MH/s	74.83	47.4
RTX 4060 8GB	4117.78 MH/s	48.61	63.8

Evaluasi kinerja komputasi pada algoritma SHA-256 melalui lima iterasi pengujian menegaskan dominasi arsitektur Ada Lovelace, di mana GeForce RTX 4060 8GB mencatatkan throughput tertinggi sebesar 4117,78 MH/s dengan latensi paling responsif di angka 48,61 ms. Capaian ini menunjukkan efisiensi eksekusi instruksi aritmatika yang superior pada beban kerja menengah. Sebaliknya, pola keterbatasan arsitektur kembali terlihat pada GeForce RTX 3050 6GB yang tertinggal signifikan dari pendahulunya, GeForce GTX 1660 Ti. Meskipun merupakan generasi yang lebih baru, RTX 3050 hanya mampu menghasilkan 2007,22 MH/s dengan latensi tertinggi 74,83 ms, kalah telak dari GTX 1660 Ti yang mampu stabil pada angka 2914,2 MH/s. Disparitas ini mengindikasikan bahwa penyempitan jalur data pada RTX 3050 menjadi penghambat utama (bottleneck) potensi core Ampere. Fenomena ini dikonfirmasi oleh profil suhu, di mana RTX 3050 beroperasi pada suhu terendah 47,4°C yang menandakan terjadinya underutilization, berbeda secara kontras dengan RTX 4060 yang menyentuh 63,8°C akibat beban kerja maksimal, serta GTX 1660 Ti yang menjaga efisiensi termal moderat pada 51,86°C.

Analisis Kinerja Komputasi Pada Algoritma Bcrypt

TABEL 3. Hasil Kinerja Komputasi Algoritma Bcrypt

Bcrypt	Hashrate	Latency (ms)	Suhu Max (°C)
GTX 1660TI 6GB	2914.2 MH/s	68.712	51.86
RTX 3050 6GB	2007.22 MH/s	74.83	47.4
RTX 4060 8GB	4117.78 MH/s	48.61	63.8

IJCSR: The Indonesian Journal of Computer Science Research
E-ISSN 2963-9174 **DOI prefix** 10.37905
Volume 5, No. 1 Januari 2026
https://subset.id/index.php/IJCSR

Evaluasi kinerja pada algoritma Bcrypt yang memiliki karakteristik komputasi intensif dan lambat menunjukkan pergeseran tren yang signifikan dibandingkan pengujian sebelumnya. Berdasarkan rata-rata lima iterasi pengujian, GeForce RTX 4060 8GB tetap mempertahankan posisi puncak dengan throughput masif sebesar 45.209,8 H/s dan latensi terendah 32,988 ms. Namun, fenomena pembalikan kinerja terjadi pada komparasi kelas menengah, di mana GeForce RTX 3050 6GB kini mampu mengungguli GeForce GTX 1660 Ti secara drastis. RTX 3050 mencatat kecepatan 24.637,4 H/s, meningkat lebih dari dua kali lipat dibandingkan GTX 1660 Ti yang tertahan di angka 10.944,4 H/s. Temuan ini menegaskan bahwa pada beban kerja yang bersifat compute-bound seperti Bcrypt, efisiensi arsitektur core Ampere memegang peranan lebih krusial dibandingkan lebar jalur memori yang sebelumnya menjadi hambatan pada algoritma ringan. Dari sisi termal, seluruh perangkat beroperasi pada suhu yang sangat rendah di bawah 46°C, dengan RTX 3050 mencatat suhu terdingin 36,22°C, mengindikasikan bahwa kompleksitas matematika Bcrypt membatasi saturasi panas yang biasanya terjadi pada algoritma berkecepatan tinggi, meskipun latensi RTX 3050 tercatat paling tinggi yakni 45,45 ms.

KESIMPULAN

Berdasarkan hasil analisis dan keterbatasan yang ditemukan selama proses penelitian, terdapat beberapa aspek strategis yang disarankan untuk dikaji pada penelitian selanjutnya guna memperkaya khazanah literatur forensik digital. Pertama, penelitian mendatang disarankan untuk memperluas cakupan objek uji dengan melibatkan arsitektur dari vendor lain, seperti AMD Radeon atau Intel Arc, guna memberikan komparasi lintas platform yang lebih holistik. Selain itu, mengingat temuan signifikan mengenai dampak lebar jalur memori (memory bus width) pada kinerja algoritma ringan, studi lanjutan sebaiknya menguji variasi algoritma Memory-Hard modern seperti Argon2 atau Scrypt, yang dirancang khusus untuk menahan serangan berbasis GPU. Hal ini penting untuk memvalidasi apakah keunggulan arsitektur terbaru (seperti Ada Lovelace) tetap konsisten pada algoritma yang resisten terhadap komputasi paralel. Kedua, disarankan untuk melakukan evaluasi kinerja pada lingkungan sistem operasi yang berbeda, khususnya distribusi Linux yang sering kali menawarkan manajemen driver dan alokasi sumber daya yang lebih efisien dibandingkan Windows untuk beban kerja server. Analisis juga dapat diperluas ke ranah komputasi awan (Cloud Computing), dengan membandingkan efisiensi biaya (cost-efficiency) antara membangun infrastruktur fisik sendiri (on-premise) melawan penyewaan instans GPU cloud. Terakhir, skenario pengujian sebaiknya tidak hanya terbatas pada mode Brute Force murni, melainkan juga mengintegrasikan metode serangan hibrida (Hybrid Attack) atau berbasis aturan (Rule-based) untuk merepresentasikan simulasi ancaman nyata yang lebih akurat dan relevan dengan tren keamanan siber terkini.

DAFTAR PUSTAKA

1. S. Vastrad and K. Naik, Comparative Analysis of Password Cracking Techniques using GPU, Int. J. Comput. Appl. 174, 15–20 (2021).
2. Z. Jia, M. Maggioni, B. Staiger, and D. P. Scarpazza, “Dissecting the NVIDIA Turing T4 GPU Architecture via Microbenchmarking,” in *arXiv preprint arXiv:1903.07486* (Cornell University, Ithaca, 2019).
3. H. Martínez, G. Olaso, and M. Valero, Energy Efficiency Analysis of NVIDIA Turing Architecture for High Performance Computing, J. Parallel Distrib. Comput. 138, 112–124 (2020).
4. J. Choquette, W. Gandhi, O. Giroux, N. Lamm, and A. Stuart, NVIDIA A100 Tensor Core GPU: Performance and Innovation, IEEE Micro 41, 29–35 (2021).
5. T. Brothers, S. Sahu, and H. Chi, Evaluating Password Cracking Performance on Cloud-Based GPU Instances, J. Cybersecur. Priv. **2**, 450–462 (2022).
6. W. Wong, Architectural Improvements in Ada Lovelace for High-Performance Computing, https://www.electronicdesign.com/technologies/embedded/article/21251345/architectural-improvements-in-ada-lovelace, diakses 26 Januari 2026.
7. NVIDIA Corporation, NVIDIA Ada Lovelace Architecture Whitepaper, https://images.nvidia.com/aem-dam/Solutions/geforce/ada/nvidia-ada-gpu-architecture.pdf, diakses 26 Januari 2026.
8. J. Sanders and E. Kandrot, CUDA by Example: An Introduction to General-Purpose GPU Programming (Addison-Wesley, Boston, 2010), pp. 15–30.

9. S. A. Manavski, "CUDA compatible GPU as an efficient hardware accelerator for AES cryptography," in Signal Processing and Communications 2007, IEEE International Conference Proceedings (IEEE, Dubai, 2007), pp. 65–68.
10. J. Steube, Hashcat: World's fastest and most advanced password recovery utility, https://hashcat.net/hashcat/, diakses 26 Januari 2026.