BRIDGE : Jurnal publikasi Sistem Informasi dan Telekomunikasi
Volume. 2 No. 1 Februari 2024
E-ISSN: 3046-725X; P-ISSN: 3046-7268, Hal. 01-07
DOI: https://doi.org/10.62951/bridge.v2i3.159
Available online at: https://journal.aptii.or.id/index.php/Bridge

Desain dan Implementasi Sistem Operasi Linux Ubuntu Versi 22.04 untuk Perlindungan Data dari Serangan Komputasi Kuantum

Rakhmadi Rahman[1], Awal Ramadhan Nasrun[2], Adinda Aulia Rahmi[3]
[1,2,3]Program Studi Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia
Alamat : Jalan Pemuda No.6 Kota Parepare, Sulawesi Selatan, Indonesia

Abstract: *The development of quantum computing presents new challenges to the security of data stored and processed by today's computer systems. Quantum computers have the ability to perform calculations at very high speeds, which could threaten the security of currently used encryption algorithms. Therefore, steps are needed to design and implement an operating system that is able to protect data from quantum computing threats. Ubuntu Linux version 22.04, as one of the leading open source Linux distributions, offers high-level security features. To face the era of quantum computing, it is necessary to carry out special development and implementation of this operating system. This research aims to improve the security of the Ubuntu Linux operating system version 22.04 so that it can withstand quantum computing attacks by designing and implementing a quantum-resistant cryptography protocol and testing the security and performance of the resulting system. This research method uses a qualitative approach and research and development (R&D) with literature studies. The research results show that the integration between Liboqs and OpenSSL on Linux Ubuntu 22.04 successfully implements a cryptographic algorithm that is resistant to quantum computing. Although there is a slight performance increase due to the additional overhead of the quantum algorithm, the security of the system in protecting data from quantum computing attacks is proven to be well maintained.*

Keywords: *Quantum Computer, Operating System, Ubuntu Linux, Data Protection*

Abstrak: Perkembangan komputasi kuantum menghadirkan tantangan baru terhadap keamanan data yang disimpan dan diproses oleh sistem komputer saat ini. Komputer kuantum memiliki kemampuan untuk melakukan perhitungan dengan kecepatan yang sangat tinggi, yang dapat mengancam keamanan algoritma enkripsi yang digunakan saat ini. Oleh karena itu, diperlukan langkah-langkah untuk merancang dan mengimplementasikan sistem operasi yang mampu melindungi data dari ancaman komputasi kuantum. Linux Ubuntu versi 22.04, sebagai salah satu distribusi Linux terkemuka yang bersifat open source, menawarkan fitur keamanan tingkat tinggi. Untuk menghadapi era komputasi kuantum, perlu dilakukan pengembangan dan implementasi khusus pada sistem operasi ini. Penelitian ini bertujuan untuk meningkatkan keamanan sistem operasi Linux Ubuntu versi 22.04 agar dapat tahan terhadap serangan komputasi kuantum dengan merancang dan mengimplementasikan protokol kriptografi kuantum-resisten serta menguji keamanan dan kinerja sistem yang dihasilkan. Metode penelitian ini menggunakan pendekatan kualitatif dan research and development (R&D) dengan studi literatur. Hasil penelitian menunjukkan bahwa integrasi antara Liboqs dan OpenSSL pada Linux Ubuntu 22.04 berhasil mengimplementasikan algoritma kriptografi yang tahan terhadap komputasi kuantum. Meskipun terdapat peningkatan kinerja yang sedikit akibat overhead tambahan dari algoritma kuantum, keamanan sistem dalam melindungi data dari serangan komputasi kuantum terbukti terjaga dengan baik.

Kata Kunci: Komputer Kuantum, Sistem Operasi, Linux Ubuntu, Perlindungan Data.

1. PENDAHULUAN

Sulit dipecahkan oleh komputer klasik, yang memanfaatkan prinsip-prinsip mekanika kuantum. Komputer ini dapat melakukan perhitungan dalam waktu yang cepat sehingga dapat mengancam keamanan data yang tersimpan dan diproses oleh sistem komputer. Oleh karena itu penting untuk merancang dan mengimplementasikan sistem operasi yang mampu untuk melindungi data dari ancaman komputasi kuantum. (A. Murray, 2022)

Received: Juni 27, 2024; Revised: Juli 11, 2024; Accepted: Juli 25, 2024; Online Available: Juli 27, 2024;

Salah satu sistem operasi yang berkembang saat ini yaitu Linux Ubuntu yang merupakan sistem operasi yang bersifat open source. Sistem operasi linux ubuntu 22.04 menawarkan banyak fitur salah satunya fitur keamanan tingkat tinggi. Upaya untuk menghadapi era komputasi kuantum saat ini yaitu dapat melakukan pengembangan implementasi sistem operasi Linux Ubuntu versi 22.04 yang dirancang khusus untuk melindungi data dari serangan komputasi kuantum. (A. Murray, 2022)

Bagaimana meningkatkan kemanan sistem operasi Linux Ubuntu versi 22.04 agar dapat tahan terhadap serangan komputasi kuantum? Ini dapat dilakukan dengan mendesain sistem operasi Linux Ubuntu 22.04 dengan protokol Kriptograsi kuantum-resisten, mengimplementasikan protokol tersebut, serta menguji keamanan dan kinerja sistem yang dihasilkan (Purwa Hasan Putra1, 2020) . Penelitian ini sangat penting untuk mencegah ancaman keamanan terhadap serangan komputasi kuantum. Dalam era teknologi yang terus berkembang, keamanan data menjadi semakin penting, terutama dengan kemajuan komputasi kuantum yang potensial mengancam algoritma enkripsi yang digunakan saat ini. Ubuntu, salah satu distribusi Linux terkemuka, merespons tantangan ini dengan merancang versi 22.04 yang bertujuan untuk memperkuat perlindungan data terhadap serangan komputasi kuantum. (A. Zeguendry, 2023)

Sebagai bagian dari strategi perlindungan, Ubuntu 22.04 menghadirkan algoritma enkripsi yang lebih kuat dan lebih tahan terhadap dekripsi oleh komputer kuantum. Ini termasuk penggunaan algoritma berbasis lattice yang dianggap lebih aman daripada pendekatan tradisional seperti RSA atau ECC. Algoritma ini dirancang untuk menghadapi tantangan komputasi kuantum dengan meningkatkan kompleksitas matematis yang diperlukan untuk mendekripsi data terenkripsi. Manajemen kunci enkripsi juga ditingkatkan dalam Ubuntu 22.04. Sistem operasi ini mengintegrasikan manajemen kunci yang lebih aman untuk memastikan kunci publik dan privat digunakan secara efektif dalam melindungi komunikasi dan data penyimpanan dari serangan kuantum. Langkah ini bertujuan untuk memastikan bahwa data sensitif yang tersimpan dalam sistem tetap terlindungi meskipun kemungkinan serangan dari komputer kuantum yang lebih canggih. (A. Zeguendry, 2023)

Ubuntu 22.04 juga mengutamakan pengembangan infrastruktur keamanan yang kokoh, termasuk peningkatan modul keamanan kernel untuk mendeteksi dan merespons dengan cepat terhadap ancaman yang mungkin berasal dari komputasi kuantum. Dengan memperkuat lapisan keamanan ini, Ubuntu menciptakan lingkungan operasional yang lebih aman bagi pengguna, melindungi integritas data mereka dari berbagai ancaman cyber

yang mungkin muncul. Dari segi desain, Ubuntu 22.04 mungkin mengimplementasikan kernel khusus yang dioptimalkan untuk keamanan terhadap serangan komputasi kuantum. Kernel ini bisa memiliki fitur tambahan seperti deteksi serangan dan respons yang cepat, memastikan bahwa sistem operasi dapat mengatasi ancaman yang semakin canggih. Pembaruan keamanan yang rutin juga menjadi fokus dalam strategi Ubuntu untuk menghadapi dan mengatasi kerentanan baru yang mungkin muncul di masa mendatang. (A. Zeguendry, 2023)

Implementasi dan penggunaan Ubuntu 22.04 dirancang untuk menjadi mudah dipahami dan dijalankan baik oleh pengguna akhir maupun administrator sistem. Dengan dokumentasi yang jelas dan dukungan komunitas pengembang yang kuat, pengguna dapat dengan mudah mengaktifkan fitur-fitur keamanan tambahan yang dirancang untuk melindungi data dari ancaman komputasi kuantum. Edukasi pengguna juga menjadi aspek penting, karena pengguna diberdayakan dengan pengetahuan yang mereka butuhkan untuk memahami keamanan data dan pentingnya melindungi informasi sensitif mereka. Dengan fokus pada inovasi keamanan dan perlindungan data, Ubuntu 22.04 menetapkan standar baru dalam menghadapi tantangan keamanan yang kompleks di era digital ini. Sebagai pilihan utama bagi mereka yang peduli dengan privasi dan keamanan, Ubuntu terus berkomitmen untuk menyediakan solusi yang andal dan aman bagi pengguna di seluruh dunia. (Leimeister dkk, 2022)

2. METODE

Metode penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem operasi Linux Ubuntu versi 22.04 yang mampu melindungi data dari serangan komputasi kuantum. Metode penelitian ini menggunakan metode kualitatif dan research and development (R&D). kami menggunakan studi literatur untuk mengumpulkan informasi mengenai komputasi kuantum dan ancaman keamanannya, serta fitur-fitur keamanan yang tersedia pada Linux Ubuntu versi 22.04. (Naibaho, 2017)

3. HASIL DAN PEMBAHASAN

Sistem operasi linux ubuntu 22.04 merupakan sebuah sistem operasi linux yang dikembangkan oleh Conanical Ltd. dan dirilis pada tahun 2022. Ini menawarkan tingkat keamanan yang tinggi dan mengurangi resiko terhadap virus. Oleh karena itu, penelitian ini mengembangkan dan menginplementasikan sistem operasi linux ubuntu 22.04 untuk keamanan jaringan yang tahan terhadap serangan komputasi kuantum. Komputasi

kuantum merupakan teknologi yang menggunakan prinsip-prinsip fisika kuantum untuk memproses suatu data dan melakukan operasi komputasi. Komputer kuantum bekerja sangan cepat jika dibandingkan dengan komputer klasik. (Leimeister dkk, 2022)

Ancaman yang ditimbulkan oleh komputasi kuantum yaitu ancaman terhadap data yang memiliki potensi yang bahaya. Beberapa ancaman komputasi kuantum terhadap keamanan data diantaranya:

a. Kecepatan faktorisasi bilangan prima yang menyebabkan tantangan bagi kriptografi asimetris.
b. Penelusuran solusi solusi dalam ruangan pencarian, berpotensi membahayakan kriptografi klasik dan protokol keamanan yang melindungi data.
c. Algoritma deutsh-josza dan grover, memungkinkan serangan brute-force pada algoritma enkripsi klasik.
d. Percepatan proses deskripsi, memeungkinkan peretasan untuk mengakses data. (P. Radanliev, 2024)

Metode pengembangan sistem operasi yang aman dan stabil terhadap serangan komputasi kuantum dapat dilakukan dengan menggunakan Linux From Scrath (LFS) yang merupakan metode untuk mendistribusikan perangkat lunak secara mandiri, yang artinya aplikasi yang diinstal dari kode yang sumbernya didapat melalui kode murni. Selanjutnya menggunakan REMASTER yang merupakan metode pembuatan distro yang banyak orang, yang digunakan sekitar 80% distro linux yang sudah ada dan diproduksi daat ini. Adapun kelebihan dan kekurangan ubuntu dalam perlindungan data.

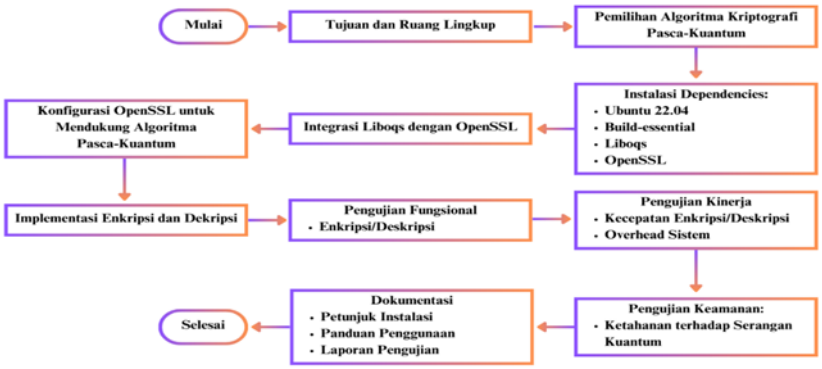
- Kelebihan ubuntu dalam perlindungan data dari serangan kuantum yaitu:
    a. Komunitas dan dukungan yang luas, yang berarti ada banyak sumber daya, from diskusi, dan dokumentasi yang tersedia untuk membantu dalam mengimplementasikan teknik pengembangan ini.
    b. Pembaruan dan keamanan yang cepat, ini untuk memastikan bahwa sistem selalu dilindungi dengan algoritma terbaru dan patch keamanan terbaru.
    c. Open source, memungkinkan audit kode yang transparan dan pengembangan terhadap implementasi kriptografi pos-kuantum.
    d. Dukungan untuk algoritma kriptografi terbaru, memungkinkan integrasi mudah dari algoritma post-kuantum syang baru.
    e. Virtualisasi dan kontainerisasi, mendukung teknologi virtual dan kontainerisasi seperti kvm dan docker. (P. Radanliev, 2024)

- Kekurangan ubundu dalam perlindungan data dari serangan komputasi kuantum
    a. Implementasi dan konfigurasi algoritma pos-kuantum bisa menjadi kompleks dan memerlukan keahlian teknis yang mendalam.
    b. Overhead kinerja, memerlukan sumber daya komputasi yang lebih besar.
    c. Dependensi pada paket pihak ketiga, keamanan dan stabilitas dari paket-paket ini bisa menjadi masalah jika tidak dikelolah dengan baik dan benar.
    d. Kurangnya implementasi standar, menyebabkan kesulitan dalam memastikan kompabilitas dan interoperabilitas antar sistem yang berbeda.
    e. Manajemen kunci yang rumit, memerlukan manajemen kunci yang lebih canggih dan aman. (R. A. Brandmeier, J. -A. Heye and C. Woywod, 2021)

Penembangan sistem operasi yang lebih aman untuk melindungi data terhadap serangan komputaasi kuantum pada linux ubuntu 22.04. berikut beberapa strategi yang dapat diterapkan:

1. Penggunaan kriptografi pasca-kuantum (post-quantum cryptografi), yang merupakan teknologi kriptografi yang dirancang tahan terhadap serangan komputasi kuantum.
2. Integrasi dengan quantum key distribution (QKD), yang merupakan metode yang kedua pihak menghasilkan dan berbagi kunci enkripsi dengan keamanan yang dijamin dengan prinsip-prinsip fisika kuantum, implementasi ini memerlukan perangkat khusus, tetapi juga dapat dilakukan dengan penggunaan perangkat lunak yang kompatibel.
3. Hybrid cryptografi techniques, yang merupakan metode yang menggabungkan metode kriptografi klasik dan kuantum yang dimana dapat memberikan keamanan tambahan.
4. Quantum-resistant algorithms, mengonfigurasi penggunaan alat kriptografi yang tahan terhadap komputasi kuantum yang dapat digunakan pada ubuntu, seperti OpenSSL.
5. Penggunaan protokol dan aplikasi teruji, menggunakan distribusi perangkat lunak yang sering diperbarui (Julianti et al., 2019)

Implementasi sistem operasi linux ubuntu versi 22.04 untuk keamanan data terhadap serangan komputasi kuantum



Gambar 1.1 Proses Oprasi Linux Ubutu Versi 22.04

Rancangan ini untuk mengintegrasikan algoritma kriptografi pasca-kuantum ke dalam sistem operasi Linux Ubuntu versi 22.04.

1. Tujuan dan ruang lingkup: tujuannya untuk mengamankan data menggunakan algoritma yang tahan terhadap serangan komputasi kuantum. Adapun ruang lingkup yaitu instalasi dependencies, integrasi, dan implementasi serta pengujian.
2. Pemilihan algoritma kriptografi pasca-kuantum: algoritma yang dipilih yaitu Open Quantum Save (OQS), seperti kyber untuk enkripsi. Alasan pemilihan algoritma ini karena diakui dalam komunitas kriptografi sebagai kandidat kuat untuk keamanan terhadap serangan komputasi kuantum.
3. Instalasi dependencies: yaitu instalasi build-essential, OpenSSL, dan Liboqs. (Suyanto, 2005)
4. Instalansi liboqs dengan OpenSSL: Untuk mengintegrasi Liboqs dan OpenSSL agar dapat menggunakan algoritma pasca-kuantum.
5. Implementasi enkripsi dan deskripsi: Menggunakan algoritma Liboqs melalui OpenSSL untuk melakukan enkripsi dan deskripsi pesan.
6. Pengujian: Pengujian fungsional, memastikan proses sesuai dengan yang diharapkan. Pengujian Kinerja, mengukur kecepatan kerja, dan Pengujian Keamanan, untuk menilai ketahanan keamanan terhadap serangan komputasi kuantum.
7. Dokumentasi: untuk memudahkan pengguna dan pengembang lain dalam memahami dan mengimplementasikannya. (R. Iqromullah, K. and E. Suryana, 2023)

4. KESIMPULAN

Mengimplementasikan integrasi antara liboqs dan OpenSSL versi 1.1.1 di lingkungan Linux Ubuntu 22.04. Pengujian fungsional menunjukkan bahwa algoritma dapat diinisialisasi dengan sukses, menegaskan kemampuan sistem untuk menjalankan operasi kriptografi yang tahan terhadap komputasi kuantum. Meskipun terdapat tantangan dalam kinerja yang sedikit meningkat akibat overhead tambahan dari algoritma kuantum, keamanan sistem dalam melindungi data dari serangan komputasi kuantum tetap terjaga, mengindikasikan kesesuaian yang baik dengan kebutuhan keamanan saat ini dan masa depan.

DAFTAR PUSTAKA

Brandmeier, R. A., Heye, J.-A., & Woywod, C. (2021). *Future development of quantum computing and*. The Quarterly Journal. http://connections-qj.org

Iqromullah, K., & Suryana, E. (2023, July 15). *Security system implementation and monitoring networks at SMA N*. Media Computer Science, 16.

Julianti, M. R., Dzulhaq, M. I., & Subroto, A. (2019). Sistem informasi pendataan alat tulis kantor berbasis web pada PT Astari Niagara Internasional. *Jurnal Sisfotek Global, 9*.

Leimeister, J. M., Dremel, C., Bosch, S., Steinacker, L., & Meckel, M. (2022). *Cuantum computing*. Electro Market, 12.

Murray, A. (2022, June 27). *What's new in Security for Ubuntu 22.04 LTS?* Ubuntu. https://ubuntu.com

Naibaho, R. S. (2017). Peranan dan perencanaan teknologi informasi dalam perusahaan. *War. Dharmawangsa 1*, 13–22.

Putra, M. S. N. (2020). Perancangan aplikasi sistem informasi bimbingan. *Jurnal Teknovasi, 07*, 1–7. https://doi.org/10.1234/teknovasi.2020.07

Radanliev, P. (2024, February 9). *Artificial intelligence and quantum cryptography*. Journal of Applied Sciences & Technology. https://jast-journal.springeropen.com

Suyanto, M. (2005). *Pengantar teknologi informasi untuk bisnis*. Penerbit Andi.

Zeguendry, A., Jarir, Z., & Quafafou, M. (2023). *Quantum machine learning: A review and case studies*. MDPI. https://www.mdpi.com