BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya teknologi dan semakin populernya informasi, kebutuhan akan media penyimpanan data yang besar juga semakin meningkat. Oleh karena itu, muncul masalah terkait bagaimana cara mendapatkan media penyimpanan yang lebih besar dan aman untuk menampung file, salah satunya melalui teknologi berbagi file dengan menggunakan protokol *Server Message Block* (SMB) (Wijaya et al., 2022). Protokol SMB memungkinkan layanan berbagi file yang memudahkan pengelolaan penyimpanan data, sementara Samba berfungsi sebagai perangkat lunak untuk implementasi SMB, yang menawarkan beberapa keunggulan, seperti sifatnya yang gratis, kemampuannya untuk terhubung langsung ke jaringan, serta kompatibilitas dengan berbagai platform yang menjadikannya pilihan populer (Insanudin et al., 2024).

Alasan utama penggunaan Linux dalam berbagi file, termasuk menggunakan protokol SMB melalui perangkat lunak Samba, adalah stabilitasnya yang tinggi, Linux dirancang sebagai sistem operasi multiuser, yang memastikan bahwa hanya pengguna dengan akses khusus seperti "root" atau "administrator" yang dapat mengakses kernel dan melakukan perubahan pada sistem. Hal ini meningkatkan tingkat keamanannya. Linux juga memiliki perlindungan yang baik terhadap virus dan malware. Meskipun tidak ada sistem yang sepenuhnya aman, sifat open source Linux memungkinkan komunitas pengguna untuk memperbaiki celah keamanan (*vulnerabilities*) dengan cepat. Semua proses, folder, dan file di Linux dapat dikontrol dan diawasi, sehingga transparansi ini menjadikannya pilihan yang sangat baik bagi para administrator. Dengan memanfaatkan protokol SMB, pengguna dapat mengelola dan membagikan data dengan mudah, aman, dan kompatibel dengan berbagai sistem operasi (Rezaldy & Ropianto, 2023).

Dalam penelitian ini, saya menggunakan protokol SMBv1. Meskipun protokol SMBv1 menawarkan banyak keunggulan, akan tetapi SMBv1 mempunyai kelemahan yang signifikan, terutama terkait dengan keamanan dan efisiensi jaringan. Protokol ini tidak menyediakan mekanisme enkripsi bawaan, sehingga data yang dikirimkan melalui SMBv1 dapat dengan mudah disadap atau dimodifikasi(Vinodhini et al., 2021). Kriptografi menjadi solusi untuk melindungi kerahasiaan data yang dikirim, dengan mengubah pesan asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) melalui enkripsi menggunakan kunci yang hanya diketahui oleh pengirim dan penerima. Dengan demikian, pihak lain yang tidak memiliki kunci tidak akan dapat membaca isi pesan tersebut (Anggraeni Eka Putri et al., 2021). Untuk mengatasi masalah keamanan ini, kombinasi algoritma enkripsi seperti AES (*Advanced Encryption Standard*) dan ChaCha20 digunakan untuk meningkatkan keamanan data selama transfer file.

AES merupakan algoritma enkripsi block cipher yang efektif dan efisien dalam mengenkripsi data dengan panjang kunci yang bervariasi (128 bit, 192 bit, dan 256 bit). Pemilihan panjang kunci ini mempengaruhi jumlah putaran enkripsi dan tingkat keamanannya (Azhari et al., 2022). Di sisi lain, ChaCha20, yang merupakan varian dari Salsa20, telah terbukti memiliki tingkat keamanan yang tinggi dan digunakan secara luas oleh Google dalam berbagai aplikasinya. Algoritma ini menggunakan keystream yang dihasilkan dari kombinasi kunci rahasia dan nonce, memastikan bahwa proses enkripsi dan dekripsi tetap aman dari potensi ancaman (Lima et al., 2022). Kombinasi kedua algoritma ini memungkinkan perlindungan data yang lebih kuat selama pertukaran informasi.

Sebagai solusi terhadap permasalahan keamanan file pada sistem penyimpanan berbagi menggunakan protokol SMB, penerapan sistem enkripsi yang menggabungkan AES Modifikasi AddRoundKey dan ChaCha20 memberikan perlindungan yang lebih tinggi. Dalam sistem ini, file yang diunggah ke Samba akan dienkripsi terlebih dahulu di server menggunakan AES untuk mengenkripsi file AES dan ChaCha20 untuk menghasilkan keystream yang aman. Setelah file terenkripsi, hanya pihak yang memiliki kunci yang sesuai yang dapat mengunduh dan membuka file tersebut. Dengan cara ini, file yang dipertukarkan melalui protokol SMB tetap terlindungi dari ancaman seperti peretasan, virus, atau

malware. Solusi ini memberikan tingkat keamanan yang lebih baik untuk file pada proses unggah dan unduh melalui protokol SMBv1 menggunakan Samba. Maka dari itu file yang diunggah akan dienkripsi setelah proses upload selesai, dan file yang diunduh akan didekripsi sebelum diterima pengguna menggunakan kombinasi algoritma ChaCha20 dan AES Modifikasi. Dengan cara ini, keamanan data selama transfer dapat lebih terjamin, memberikan perlindungan tambahan terhadap risiko penyadapan atau manipulasi data serta dapat menyimpan file di file sharing dengan aman bagi pengguna dalam berbagi data di platform Linux.

1.2 Rumusan Masalah

1. Bagaimana implementasi kombinasi algoritma enkripsi ChaCha20 dan modifikasi AES untuk enkripsi *file* pada proses *upload* dan *download* melalui Protokol SMB?
2. Bagaimana implementasi proses dekripsi *file* setelah di*download* menggunakan kombinasi algoritma ChaCha20 dan modifikasi AES melalui Protokol SMB?
3. Bagaimana evaluasi keamanan dari implementasi enkripsi dan dekripsi kombinasi ChaCha20 dan AES yang dimodifikasi dalam proses berbagi file melalui Protokol SMB?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menerapkan kombinasi algoritma enkripsi ChaCha20 dan AES yang dimodifikasi untuk proses enkripsi file selama upload dan download melalui Protokol SMB, dengan tujuan meningkatkan keamanan data yang dibagikan.
2. Menganalisis proses dekripsi file yang telah dienkripsi menggunakan kombinasi algoritma ChaCha20 dan AES yang dimodifikasi, setelah diunduh melalui Protokol SMB, untuk memastikan keamanan, integritas, dan akurasi data yang dibagikan.
3. Mengevaluasi dampak dari penerapan kombinasi algoritma ChaCha20 dan modifikasi AES terhadap *performa* Protokol SMB dalam proses berbagi *file*, untuk mengetahui seberapa besar pengaruhnya terhadap kinerja sistem.

1.4 Batasan Masalah

1. Penelitian ini hanya akan menguji dan menerapkan sistem enkripsi pada *file* teks format (pdf, docx, xlsx, txt) serta *file* gambar format (jpg, jpeg dan png) dengan ukuran 10KB-100MB. Pemilihan format ini didasarkan pada karakteristik *file* yang umum digunakan, representasi data yang berbeda (teks dan biner), serta kemudahan akses dan pengujian algoritma enkripsi dan dekripsi.
2. Penelitian ini akan fokus pada penggunaan protokol *Server Message Block* (SMB) v1 melalui Samba untuk berbagi *file*. Samba dipilih karena merupakan implementasi SMB yang populer pada platform Linux. Penelitian ini tidak akan membahas implementasi protokol berbagi *file* lainnya, seperti FTP atau NFS.
3. Sistem enkripsi yang diterapkan dalam penelitian ini menggunakan kombinasi algoritma ChaCha20 dan modifikasi AES (*Advanced Encryption Standard*) melalui *AddRoundKey*. Penelitian ini hanya akan menggunakan kedua algoritma ini untuk mengenkripsi dan mendekripsi data, dan tidak akan membahas atau membandingkan algoritma enkripsi lainnya.
4. Penelitian ini mengasumsikan bahwa sistem berbagi *file* menggunakan platform Linux dengan Samba sebagai alat implementasi protokol SMBv1. Sistem operasi dan perangkat keras lainnya tidak menjadi fokus penelitian, sehingga interoperabilitas pada platform selain Linux tidak akan dibahas.
5. Penelitian ini akan menguji keamanan proses enkripsi dan dekripsi data dengan melakukan analisis lalu lintas data menggunakan Wireshark. Pengujian ini dilakukan untuk memastikan bahwa data yang ditransfer melalui Protokol tetap terenkripsi pada proses transfer *file* dan terlindungi dari ancaman penyadapan (*sniffing*). Penelitian ini tidak akan membahas atau mengatasi ancaman lain di luar pengujian lalu lintas data, seperti manipulasi data atau serangan lanjutan setelah data disadap.
6. Evaluasi *performa* Samba dalam penelitian ini dilakukan berdasarkan waktu yang dibutuhkan untuk proses *upload* dan *download* selama berbagi *file* menggunakan Samba. Faktor-faktor lain yang dapat memengaruhi

performa, seperti penggunaan jaringan, sumber daya perangkat keras, atau konfigurasi Samba lainnya, tidak akan dibahas secara mendalam.

1.5 Manfaat Penelitian

1. Manfaat untuk Pengembangan Teknologi

   Penelitian ini dapat mendorong pengembangan lebih lanjut dalam hal implementasi kriptografi untuk sistem berbagi *file*. Dengan memanfaatkan kombinasi algoritma enkripsi yang aman, diharapkan dapat membuka peluang untuk menciptakan sistem berbagi *file* yang lebih aman dan dapat diandalkan di berbagai sektor, seperti pemerintahan, perusahaan, dan instansi pendidikan.

2. Manfaat Akademik

   Penelitian ini memberikan pemahaman yang lebih dalam mengenai penerapan kombinasi algoritma enkripsi ChaCha20 dan modifikasi AES dalam sistem berbagi *file* menggunakan Samba. Hasil penelitian ini diharapkan dapat memperkaya literatur di bidang kriptografi, khususnya dalam penerapan enkripsi untuk melindungi data yang dibagikan melalui protokol SMB. Penelitian ini juga dapat menjadi referensi bagi penelitian lanjutan yang mengkaji keamanan data dalam sistem berbagi *file* berbasis Linux.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini memuat teori-teori pendukung dan kajian pustaka yang relevan dengan topik penelitian, seperti konsep dasar protokol SMB, kriptografi, algoritma AES, ChaCha20, serta penelitian terdahulu terkait keamanan file.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan langkah-langkah dalam pelaksanaan penelitian, mulai dari alur penelitian, alat dan bahan, perancangan sistem, implementasi algoritma, pengujian, dan evaluasi performa sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi sistem, pengujian performa dan keamanan, serta analisis terhadap pengaruh penggunaan kombinasi algoritma ChaCha20 dan modifikasi AES dalam sistem file sharing berbasis Samba.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan dan saran untuk pengembangan atau penelitian selanjutnya.