BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya perkembangan teknologi terutama dalam penggunaan internet dan transaksi online membuat risiko terhadap pencurian data, kerusakan data, dan pemalsuan data oleh pihak tidak bertanggung jawab semakin meningkat (Joseph dkk., 2023), sehingga *developer* aplikasi harus lebih memperhatikan keamanan data dari aplikasi yang mereka buat dengan menerapkan metode dan algoritma keamanan guna memastikan data tidak berubah dan tidak dicuri oleh orang lain. Salah satu kasus kebocoran data pegawai baru-baru ini melibatkan lembaga pemerintah yaitu Kejaksaan RI dan dilaporkan oleh berbagai sumber berita. Hal tersebut menunjukkan bahwa keamanan data di instansi pemerintahan masih memiliki celah yang bisa dimanfaatkan oleh peretas. *Lembaga Riset Keamanan Siber Communication & Information System Security Research Center (CISSReC)* mengungkapkan bahwa data sebesar 500MB yang diretas dan diunggah ke platform daring oleh peretas, berisi informasi penting seperti email, nama, ID pegawai, dan jabatan pegawai. Pakar keamanan siber menyatakan bahwa selain risiko pencurian data, ada kemungkinan data tersebut bisa dimanipulasi oleh pihak tidak bertanggung jawab (CNN Indonesia, 2021). Menanggapi hal tersebut, maka sistem informasi tugas belajar perlu peningkatan keamanan dengan menggunakan *cryptosystem*, terutama pada *database*, sehingga apabila database diretas, peretas tidak akan bisa mengidentifikasi isi dan informasi yang ada dalam *database*.

Penelitian mengenai penerapan algoritma RSA dan AES dalam sistem informasi tugas belajar pegawai Universitas Diponegoro berbasis hashchain memiliki urgensi penting untuk memastikan keamanan dan privasi data. Permasalahan utama adalah belum adanya mekanisme kriptografi *hybrid* yang terintegrasi dengan *hashchain*, sementara sebagian besar sistem masih mengandalkan autentikasi sederhana sehingga rentan terhadap manipulasi dan kebocoran informasi. Penelitian ini bertujuan mengembangkan model keamanan

berbasis hashchain yang mengintegrasikan algoritma RSA dan AES untuk meningkatkan keamanan data transaksi melalui enkripsi hybrid dan verifikasi integritas. Sebagai institusi dengan jumlah pegawai yang besar, UNDIP mengelola data tugas belajar yang bersifat sensitif sehingga memerlukan tingkat keamanan tinggi. Meskipun masalah keamanan sering terjadi pada level pengguna (Venugopal & Kolluru, 2024), penelitian ini difokuskan pada penguatan di level kriptografi karena pendekatan ini mampu memberikan perlindungan menyeluruh terhadap data meskipun terjadi kompromi pada sisi pengguna.

Dalam sistem informasi pegawai UNDIP berbasis *hashchain*, penggunaan kombinasi algoritma *RSA* dan *AES* sebagai *cryptosystem* dapat memberikan tingkat keamanan dan privasi yang lebih tinggi pada data dibandingkan kombinasi algoritma *Twofish* dan *ElGamal* (Jintcharadze & Iavich, 2020). Algoritma Twofish adalah algoritma kriptografi simetrik yang dirancang untuk menggantikan DES dengan kecepatan tinggi dan tingkat keamanan yang lebih baik. Algoritma ini menggunakan ukuran blok 128-bit dan dapat mendukung kunci hingga 256-bit (Gaur dkk., 2019). Di sisi lain, algoritma ElGamal adalah salah satu algoritma kriptografi asimetris yang menggunakan teori logaritma diskret untuk enkripsi dan dekripsi data, yang sering diterapkan dalam komunikasi (Adeniyi dkk., 2022).

Algoritma *RSA* adalah algoritma kriptografi asimetris yang memastikan bahwa hanya pihak yang berwenang dapat mengakses data melalui proses aman pertukaran kunci (Al-Kadei dkk., 2020). Sementara itu, algoritma *AES* digunakan untuk mengenkripsi data dengan memecahnya menjadi blok, memungkinkan hanya pengguna dengan kunci yang tepat yang dapat mengakses data tersebut (Dr Asha Ambhaikar, 2021). Penggunaan kriptografi *hybrid* dengan algoritma *RSA* dan *AES* memberikan keuntungan signifikan karena menggabungkan keunggulan kriptografi simetris dan asimetris (Jaspin dkk., 2021). Teknologi *hashchain* digunakan sebagai struktur *database* yang memastikan setiap blok data memiliki nilai *hash* yang dihasilkan dari nilai hash blok sebelumnya dan data pada blok saat ini, sehingga sulit untuk dimanipulasi (Smith dkk., 2022).

Penelitian terdahulu telah menunjukkan manfaat penggunaan teknologi *hashchain* dan kriptografi *hybrid*. Studi oleh Al-Kadei dkk. (2020) mencatat

pentingnya teknik enkripsi kombinasi untuk memastikan keamanan data. Jintcharadze & Iavich (2020) menyoroti bahwa penggabungan algoritma enkripsi simetris dan asimetris dapat meningkatkan keamanan data. Penelitian lainnya oleh Dr Asha Ambhaikar (2021) menggarisbawahi efisiensi enkripsi data menggunakan *AES*, sementara Jaspin dkk. (2021) mendemonstrasikan bahwa kombinasi *RSA* dan *AES* memberikan perlindungan yang kuat terhadap serangan siber. Smith dkk. (2022) menegaskan bahwa *hashchain* efektif dalam mendeteksi dan mencegah manipulasi data dalam sistem terdistribusi, memastikan integritas data tetap terjaga. Dalam penelitian Veronika dkk. (2010) menunjukkan kombinasi *RSA* dan *AES* dalam menjamin kerahasiaan dan otentikasi data dalam komunikasi digital. Pendekatan tersebut dikembangkan lebih lanjut untuk mengamankan data transaksi dalam sistem *hashchain*, dengan menambahkan mekanisme pembangkitan kunci *AES* dari blok sebelumnya guna memperkuat keterkaitan antar blok dan meningkatkan integritas data secara keseluruhan.

Hashchain digunakan sebagai struktur *database* untuk menyimpan data di dalam sistem. Dalam *hashchain*, setiap blok data memiliki nilai *hash* yang dihasilkan dari nilai *hash* blok sebelumnya dan data pada blok saat ini. Hal ini membuat *hashchain* sulit dimanipulasi karena setiap perubahan pada blok data akan menghasilkan nilai *hash* yang berbeda, sehingga memungkinkan sistem untuk mendeteksi manipulasi data atau serangan siber yang mencoba mengubah isi blok. *RSA* dan *AES* yang digunakan pada penelitian ini menggunakan kunci sepanjang 128-bit dengan pembangkitan kunci simetris dari *password* pengguna menggunakan *default* kriptografi *AES* yaitu *pbkdf2*.

Data yang diamankan menggunakan *cryptosystem* merupakan data transaksi setiap penerima tugas belajar. Secara umum dalam penelitian ini data transaksi akan dienkripsi mengunakan kriptografi *AES* menggunakan kunci yang telah dibangkitkan menggunakan *pbkdf2,* kemudian kunci *AES* akan dienkripsi menggunakan kunci-publik *RSA* dan disimpan dalam objek *hashchain*, dari *hashchain* tersebut akan dibangkitkan kunci *AES* untuk proses selanjutnya di blok kedua dan seterusnya. Proses ini dinilai dapat memperbaiki kelemahan dari

algoritma *AES* dan *RSA* serta meningkatkan integritas data karena menggunakan *hashchain* yang saling terikat satu sama lain.

Pendekatan ini memiliki keterbaruan karena mengintegrasikan tiga mekanisme keamanan sekaligus, yaitu kriptografi hybrid (AES dan RSA), pembangkitan kunci dinamis berbasis *pbkdf2*, dan struktur *hashchain* yang saling terikat antar blok. Tidak hanya mengamankan data transaksi melalui enkripsi simetris AES dan pengamanan kunci dengan RSA, penelitian ini juga memperkuat integritas data dengan memanfaatkan *hashchain* yang di verifkasi oleh *merkle tree*, di mana setiap blok menghasilkan kunci AES untuk blok berikutnya. Mekanisme ini menciptakan keterkaitan kriptografis antar blok, sehingga mampu mendeteksi manipulasi data secara otomatis.

Pengujian sistem informasi sangat penting untuk memastikan kinerja, keamanan, dan keandalan fungsi-fungsi dalam sistem. Penggunaan *Big O Notation*, seperti ditunjukkan oleh Kumar dan Dutta (2022), penting dalam analisis efisiensi algoritma untuk menentukan kompleksitas waktu dan ruang, yang relevan untuk aplikasi tertentu. Selain itu, penerapan *merkle tree* dalam teknologi *hashchain* digunakan untuk menilai kemampuan sistem dalam menjaga integritas dan keamanan data. Studi oleh Kuznetsov dkk. (2024) dalam jurnal *Internet of Things* menunjukkan bahwa *merkle tree* dapat digunakan untuk verifikasi data dengan cepat dan efisien, memastikan bahwa tidak ada manipulasi pada data selama proses penyimpanan dan verifikasi. Teknik pengujian *blackbox*, sesuai dengan survei yang dilakukan oleh Batra dan Rishi (2011), berfokus pada input dan output sistem untuk memastikan fungsionalitas sesuai spesifikasi tanpa melihat kode internal.

Penggunaan teknik *Big O Notation* untuk menilai efisiensi dan kompleksitas algoritma, penggunaan *merkle tree* untuk menjaga integritas data, serta pengujian *blackbox* untuk validasi fungsionalitas, bertujuan mengembangkan sistem informasi tugas belajar pegawai UNDIP yang aman, efisien, dan andal. Dengan demikian, sistem ini diharapkan mampu memberikan perlindungan data yang kuat, mengidentifikasi upaya manipulasi data, serta memastikan kinerja sistem tetap optimal dalam berbagai kondisi operasional.

1.2 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai dalam penelitian ini antara lain:

1. Menganalisis kombinasi algoritma *RSA* dan *AES* berdasarkan tingkat kompleksitas dalam meningkatkan kemanan sistem informasi tugas belajar UNDIP.
2. Menganalisis tingkat efisiensi dan integritas algoritma RSA dan AES dalam sistem informasi tugas belajar Universitas Diponegoro berbasis hashchain dilakukan dengan mengukur waktu pemrosesan serta kemampuan sistem dalam mendeteksi manipulasi data, guna memastikan keandalan dan keamanan sistem secara menyeluruh.
3. Mengevaluasi performa sistem melalui pengujian fungsionalitas, efisiensi, dan integritas data menggunakan metode *blackbox testing*, analisis waktu eksekusi, serta verifikasi integritas berbasis struktur *Merkle Tree* untuk memastikan keandalan sistem informasi tugas belajar.
4. Mengembangkan model keamanan berbasis *hashchain* yang mengintegrasikan algoritma kriptografi *RSA* dan *AES*, yang dapat dijadikan sebagai referensi dalam pengembangan sistem informasi lainnya, melalui pemodelan arsitektur sistem, implementasi algoritma kriptografi, serta pengujian efektivitas dan kinerjanya.

1.3 Manfaat Penelitian

Manfaat yang ingin dihasilkan dalam penelitian ini antara lain:

1. Penerapan algoritma *RSA* dan *AES* dalam sistem informasi tugas belajar pegawai di Universitas Diponegoro dapat meningkatkan tingkat keamanan sistem, sehingga sistem menjadi lebih tangguh terhadap upaya peretasan atau penyusupan oleh pihak yang tidak berwenang.
2. Penelitian dengan algoritma *RSA* dan *AES* dalam sistem informasi tugas belajar pegawai UNDIP berbasis *hashchain* dapat meningkatkan keamanan sistem informasi dalam sisi integritas data, sehingga menjadi lebih aman dan sulit untuk diretas atau disusupi oleh pihak yang tidak berwenang.

3. Penelitian ini dapat menjadi acuan bagi pengembangan sistem informasi lainnya yang menggunakan teknologi *blockchain* dan algoritma kriptografi dalam pengamanan dan pengolahan data.