Volume 7 Nomor 1 Januari 2025 JJEEE e-ISSN : 2715-0887
p-ISSN : 2654-7813

Jambura Journal of Electrical and Electronics Engineering

Penerapan Enkripsi Hibrida AES-RSA untuk Meningkatkan Keamanan Layanan Sistem Informasi Distribusi Slip Gaji

Implementing AES-RSA Hybrid Encryption to Enhance the Security of Salary Slip Distribution Information System

Riska Kurniyanto Abdullah*
Program Studi Informatika
Institut Teknologi Kalimantan
Balikpapan, Indonesia
riska.abdullah@lecturer.itk.ac.id*

Nur Fajri Azhar
Program Studi Informatika
Institut Teknologi Kalimantan
Balikpapan, Indoneseia
fajri@lecturer.itk.ac.id

Syamsul Mujahidin
Program Studi Informatika
Institut Teknologi Kalimantan
Balikpapan, Indoneseia
syamsul@lecturer.itk.ac.id

Richard Owen Hoan
Program Studi Informatika
Institut Teknologi Kalimantan
Balikapapan, Indonesia
richardowen2411@gmail.com

Diterima : Desember 2024
Disetujui : Desember 2024
Dipublikasi : Januari 2025

***Abstrak*—Penelitian ini bertujuan untuk meningkatkan keamanan dan efisiensi dalam pendistribusian slip gaji secara digital. Metode yang diusulkan yaitu memadukan enkripsi hibrida menggunakan algoritma (*Advanced Encryption Standard*) AES-128 dan (*Rivest–Shamir–Adleman*) RSA, serta mengintegrasikan *Time-Based One-Time Password* (TOTP) sebagai autentikasi dua faktor. Pendekatan ini memastikan kerahasiaan data sensitif, sekaligus meminimalkan potensi kebocoran atau akses tidak sah terhadap informasi gaji karyawan. Dalam implementasinya, sistem dirancang menggunakan kerangka kerja *Laravel* dan metodologi pengembangan perangkat lunak *Scrum*, sehingga memungkinkan proses pengembangan yang iteratif, terukur, dan mudah diadaptasi. Hasil pengujian menunjukkan bahwa sistem dapat mendistribusikan slip gaji dengan rata-rata waktu enkripsi data sebesar 0,15 milidetik per slip (menggunakan AES-128) dan waktu dekripsi kunci AES menggunakan RSA rata-rata 5 milidetik per operasi, pada skenario 100 percobaan. Selain itu, saat pengujian autentikasi dua faktor (TOTP) diterapkan, tingkat kegagalan akses tidak sah menurun hingga 0% pada 50 percobaan simulasi serangan *bruteforce*. Dengan demikian, enkripsi hibrida terbukti efektif dalam menjaga integritas data, dan integrasi TOTP meningkatkan tingkat keamanan autentikasi pengguna. Hasil kuantitatif ini dapat dijadikan sebagai model acuan yang lebih terukur bagi institusi lain yang ingin mengelola data sensitif secara aman, dan andal.**

Kata Kunci*— *Slip gaji; enkripsi hibrida; AES-128; RSA; TOTP; keamanan data.

Abstract*— *This study aims to enhance security and efficiency in the digital distribution of salary slips within the XYZ Higher Education environment. The proposed method combines hybrid encryption using the Advanced Encryption Standard (AES-128) and Rivest–Shamir–Adleman (RSA) algorithms, as well as integrates Time-Based One-Time Password (TOTP) for two-factor authentication. This approach ensures the confidentiality of sensitive data while minimizing the potential for data leakage or unauthorized access to employee salary information. In its implementation, the system is designed using the Laravel framework and the Scrum software development methodology, enabling an iterative, measurable, and easily adaptable development process. Testing results indicate that the system can distribute salary slips with an average data encryption time of 0.15 milliseconds per slip (using AES-128), and an average AES key decryption time with RSA of 5 milliseconds per operation over 100 test iterations. Furthermore, when two-factor authentication (TOTP) was applied, the rate of unauthorized access attempts dropped to 0% across 50 brute force attack simulation attempts. Thus, the hybrid encryption approach is proven effective in maintaining data integrity, and the integration of TOTP enhances user authentication security. These quantitative findings establish the system as a more measurable reference model for other institutions seeking to manage sensitive data securely, efficiently, and reliably.

Keywords*— *Salary slip; hybrid encryption; AES-128; RSA; TOTP; data security.

I. PENDAHULUAN

Sistem informasi pengelolaan penggajian telah menjadi komponen krusial bagi institusi pendidikan tinggi, termasuk perguruan tinggi negeri maupun swasta. Proses distribusi slip gaji secara manual kerap menimbulkan kendala dalam efisiensi, transparansi, serta keamanan data sensitif [1] [2]. Seiring meningkatnya ancaman keamanan siber, kebutuhan akan solusi digital yang aman dan efektif semakin mendesak [3] [4]. Proses manual yang memakan waktu, penggunaan kertas yang berlebihan, serta potensi keterlambatan dan kesalahan dalam pendistribusian tidak hanya menghambat efisiensi, tetapi juga menimbulkan risiko keamanan. Data gaji termasuk kategori informasi sensitif yang dapat disalahgunakan jika jatuh ke tangan pihak tidak berwenang. Oleh karena itu, kebutuhan akan solusi digital yang aman, efisien, dan andal menjadi sangat relevan untuk institusi pendidikan. Dengan menerapkan sistem distribusi slip gaji berbasis web yang terintegrasi dengan metode enkripsi canggih, institusi dapat menghemat waktu, mengurangi biaya, mempermudah akses bagi para pegawai, sekaligus meningkatkan kerahasiaan data gaji mereka. Salah satu

tantangan utama dalam meningkatkan keamanan sistem informasi terletak pada manajemen kunci enkripsi. Meskipun algoritma enkripsi simetris seperti AES dapat mengenkripsi data dengan cepat dan efisien, pertukaran kunci rahasia antara pihak pengirim dan penerima menjadi titik lemah. Jika kunci ini tidak didistribusikan dengan aman, penyerang dapat mencegat atau memperoleh kunci tersebut, kemudian mendekripsi data sensitif dengan mudah. Tantangan tersebut diperparah oleh fakta bahwa institusi pendidikan sering kali memiliki infrastruktur yang tersebar (misalnya, beberapa kampus atau unit kerja berbeda), serta pegawai yang mengakses sistem dari berbagai lokasi. Hal ini mempersulit proses pengelolaan kunci enkripsi secara manual.

Sebagai contoh konkret, bayangkan sebuah institusi pendidikan yang memiliki ratusan dosen dan staf yang tersebar di berbagai departemen. Slip gaji perlu didistribusikan secara rutin setiap bulan. Jika institusi hanya mengandalkan enkripsi simetris, pengelola sistem harus mengirim kunci rahasia ke setiap penerima. Dalam proses ini, beberapa kemungkinan risiko muncul, seperti kunci rahasia tercegat oleh pihak ketiga saat dikirim melalui email, atau kunci disimpan sembarangan di komputer personal tanpa perlindungan. Situasi ini memperbesar peluang kebocoran data. Oleh karena itu, penelitian ini menggunakan pendekatan enkripsi hibrida yang memadukan AES dengan RSA. Dengan RSA, kunci AES dapat dienkripsi menggunakan kunci publik penerima, sehingga hanya penerima yang memiliki kunci privat RSA dapat mendekripsi kunci AES tersebut. Pendekatan ini secara signifikan mengurangi risiko terkait distribusi kunci, karena kunci publik dapat dibagikan secara terbuka tanpa mengurangi keamanan, sementara kunci privat milik penerima tetap aman dan tidak pernah diungkapkan. Melalui pemilihan algoritma enkripsi yang tepat dan integrasi autentikasi dua faktor berbasis Time-Based One-Time Password (TOTP), penelitian ini berupaya memberikan solusi yang dapat meningkatkan efisiensi pendistribusian slip gaji, mengurangi risiko kebocoran data, serta menyederhanakan pengelolaan kunci enkripsi. Sebagai hasilnya, institusi pendidikan dapat mengadopsi sistem yang tidak hanya mengurangi beban kerja administratif, tetapi juga menjaga kepercayaan dan kenyamanan para pegawai dengan menjamin keamanan informasi gaji mereka.

Dalam konteks keamanan data, metode enkripsi memainkan peran sentral untuk menjamin kerahasiaan informasi gaji. Menurut [5] [6] Algoritma enkripsi simetris seperti AES telah terbukti memberikan kinerja yang andal dalam hal kecepatan enkripsi. Namun, tantangan muncul dalam mendistribusikan kunci enkripsi secara aman. Untuk mengatasi hal ini, algoritma asimetris RSA dapat dimanfaatkan dalam mengelola kunci publik dan privat. Pendekatan hibrida yang menggabungkan AES dan RSA memungkinkan peningkatan keamanan tanpa mengorbankan efisiensi, terutama dalam mengamankan data gaji dalam jumlah besar [7]-[10].

Selain aspek teknis kriptografi, autentikasi juga menjadi fokus penting. Otentikasi satu faktor berbasis kata sandi tidak lagi memadai untuk menghadapi ancaman seperti *brute force* dan *phishing*. Oleh karena itu, penerapan autentikasi multi-faktor (MFA) menjadi solusi yang relevan. Penggunaan *Time-Based One-Time Password* (TOTP) sebagai faktor tambahan telah banyak dibahas dalam penelitian terkait keamanan informasi, khususnya pada sistem yang membutuhkan perlindungan data tingkat lanjut [11] [12].

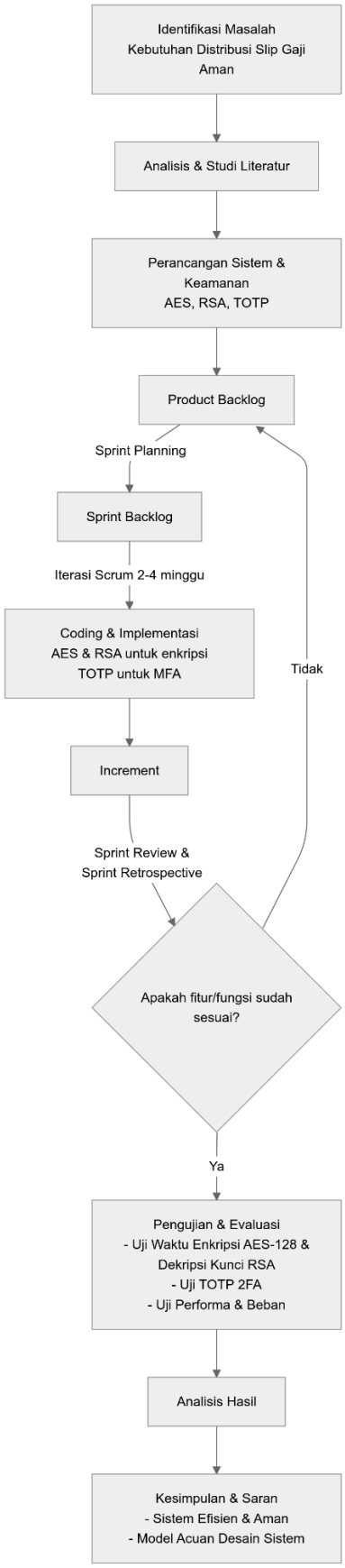
Dari sisi metodologi pengembangan, pendekatan *Agile* seperti *Scrum* serta pemanfaatan kerangka kerja (*framework*) modern, misalnya *Laravel*, mendukung proses pengembangan yang iteratif, adaptif, dan responsif terhadap perubahan kebutuhan [13]-[17]. Dengan demikian, integrasi antara metodologi pengembangan yang tepat, enkripsi hibrida (AES-RSA), serta MFA berbasis TOTP diharapkan dapat menjawab tantangan keamanan, efisiensi, dan skalabilitas dalam distribusi slip gaji secara digital.

Penelitian terdahulu terkait enkripsi hibrida telah menunjukkan bahwa gabungan AES dan RSA efektif untuk mengamankan data di lingkungan komputasi awan [7] [8]. Meski demikian, belum banyak studi yang secara khusus membahas distribusi slip gaji. Penelitian lain menekankan pada efisiensi enkripsi ganda dalam meningkatkan keamanan data [9] [10]. Sementara itu, terkait MFA, beberapa studi menekankan pentingnya lapisan autentikasi tambahan seperti TOTP untuk mencegah akses tidak sah [11] [12]. Pada sistem penggajian berbasis web, peneliti lain telah mengembangkan sistem informasi penggajian tanpa fokus khusus pada kriptografi tingkat lanjut [1]. Ada pula penelitian yang menggunakan AES 128 dalam mengamankan data berbasis web, namun belum mengadopsi pendekatan hibrida AES-RSA dan MFA [2].

Berdasarkan latar belakang tersebut, dapat dirumuskan masalah yaitu (1)Bagaimana membangun sistem distribusi slip gaji digital yang aman dengan memanfaatkan enkripsi hibrida (AES-RSA) guna melindungi data sensitif. (2)Bagaimana mengintegrasikan autentikasi multi-faktor berbasis TOTP dalam sistem distribusi slip gaji untuk meningkatkan keamanan akses. (3)Bagaimana penerapan metodologi pengembangan perangkat lunak (misalnya *Scrum*) dan pemanfaatan *framework* (*Laravel*) dapat mendukung efisiensi dan adaptabilitas sistem.

II. METODE

Dalam penelitian ini, metode yang digunakan berfokus pada perancangan, pengembangan, dan pengujian sistem distribusi slip gaji digital yang aman, adaptif, dan efisien. Pendekatan yang diterapkan mencakup pemilihan algoritma enkripsi hibrida, integrasi autentikasi multi-faktor (MFA) berbasis TOTP, serta penerapan metodologi pengembangan perangkat lunak *Agile*, khususnya *Scrum*. Selain itu, pemilihan kerangka kerja pengembangan aplikasi web berbasis PHP seperti *Laravel* dipilih untuk meningkatkan produktivitas dan konsistensi pengembangan sistem.



Gambar 1. Scrum Framework Penelitian

A. Metodologi Pengembangan Perangkat Lunak

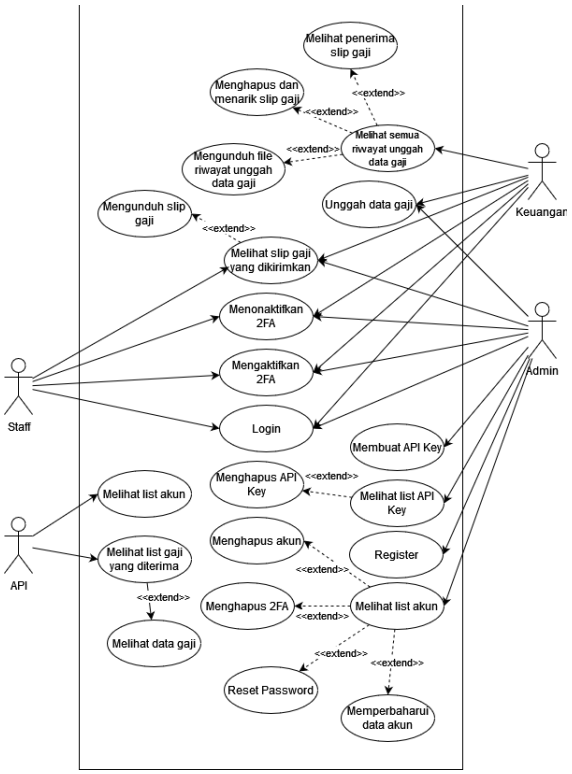
Gambar 1 Pada tahap awal, proses dimulai dengan Identifikasi Masalah dan Analisis Kebutuhan, di mana alasan dan urgensi pembangunan sistem distribusi slip gaji yang aman dirumuskan dengan jelas kebutuhannya. Pada tahap ini terdeteksi masalah efisiensi dan keamanan saat prosedur manual digunakan. Selanjutnya setelah itu, tahap Studi Literatur dan Perancangan Sistem dilakukan untuk menemukan solusi teknis yang tepat. Pemilihan AES-128 sebagai algoritma enkripsi simetris didasarkan pada kemampuannya dalam mengenkripsi data slip gaji secara cepat dan efisien, sementara RSA digunakan untuk mengamankan kunci AES tersebut. Selain itu, penerapan TOTP diusulkan untuk autentikasi dua faktor, sehingga keamanan akses pengguna meningkat secara signifikan. Hasil analisis kebutuhan kemudian diintegrasikan dengan metode Scrum. Seluruh fitur yang dibutuhkan, seperti implementasi enkripsi AES-RSA, integrasi TOTP, halaman unggah dan unduh slip gaji, dimasukkan ke dalam *Product Backlog*. Melalui proses *Sprint Planning*, ditektukan item backlog mana yang akan dikerjakan dalam satu Sprint (rentang 2-4 minggu). Pada tahap ini, dimulai untuk mengimplementasikan fitur-fitur sesuai backlog, termasuk mekanisme enkripsi hibrida dan TOTP. Di akhir setiap Sprint, dihasilkan *Increment*, yang mana tahap ini merupakan fitur yang sudah berfungsi dan siap dievaluasi.

Selanjutnya, hasil yang dicapai dipresentasikan pada *Sprint Review*. Apabila terdapat umpan balik atau perbaikan yang perlu dilakukan, maka pada *Sprint Retrospective* akan dibahas penyesuaian untuk Sprint berikutnya. Setelah fitur-fitur kunci dianggap siap, penelitian berlanjut ke tahap Pengujian dan Evaluasi. Di sini, dilakukan pengukuran waktu enkripsi data dengan AES-128, waktu dekripsi kunci AES dengan RSA, serta uji keberhasilan TOTP dalam mencegah akses tidak sah. Pengujian beban juga dilakukan untuk memastikan sistem tetap responsif jika jumlah data slip gaji bertambah.

Apabila hasil pengujian menunjukkan bahwa sistem memenuhi kriteria keamanan dan efisiensi yang diharapkan, proses penelitian ditutup dengan penarikan Kesimpulan dan Saran. Pada tahap ini, disusun rekomendasi pengembangan lebih lanjut untuk meningkatkan sistem, sehingga dapat menjadi acuan bagi institusi lain yang ingin menerapkan solusi serupa.

Proses kerangka kerja *Scrum* telah terbukti efektif dalam mengakomodasi perubahan kebutuhan dan iterasi pengembangan yang berkelanjutan [13] [16]. Pemilihan *Scrum* didukung oleh literatur yang menunjukkan keunggulannya dalam proyek-proyek kompleks dan dinamis [13], serta hasil kajian sistematis yang membandingkan berbagai metode *Agile* [16].

Di samping itu, pemanfaatan Laravel sebagai framework pengembangan web dilakukan untuk mempermudah penerapan pola MVC (Model-View-Controller), pengelolaan database, routing, serta integrasi API [14]. Laravel dipilih atas dasar hasil studi kasus yang menunjukkan fleksibilitas, efisiensi, serta kemudahan dalam pengembangan aplikasi skala kecil hingga menengah [14]. Penggunaan metode pengembangan perangkat lunak yang terstruktur dan alat bantu modern ini diharapkan dapat meningkatkan keterbacaan, pemeliharaan, serta skalabilitas sistem [15].



Gambar 2. Use Case Diagram

Desain Sistem yang dirancang memiliki fitur seperti yang ada pada Gambar 2. Fitur antara lain secara garis besar dapat membuat data yang ada pada tabel basis data yang digunakan terenkripsi semua sehingga data tidak bisa diakses secara langsung pada *database*. Dalam hal ini meskipun tim developer sendiri tidak bisa melihat data gaji yang terekam pada sistem.

B. AES-128 dan RSA

Algoritma AES-128 merupakan algoritma enkripsi simetris berbasis blok dengan panjang kunci 128 bit dan panjang blok 128 bit yang bekerja melalui beberapa putaran transformasi, meliputi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*, untuk mengubah *plaintext* menjadi *ciphertext* [5] [6]. Tidak terdapat satu persamaan tunggal yang mewakili AES, karena ia merupakan serangkaian operasi linier dan non-linier pada blok data. Sementara itu, RSA adalah algoritma asimetris yang bergantung pada pasangan kunci publik dan privat. Dalam RSA, jika M adalah *plaintext*,
C *ciphertext*, (n,e) kunci publik, dan (n,d) kunci privat, maka proses enkripsi didefinisikan pada rumus 1, dan proses dekripsi pada rumus 2

$$C \equiv M^e \ (mod\ n) \ldots . (1)$$

$$M \equiv C^d \ (mod\ n) \ \ldots (2)$$

C. Pemilihan dan Implementasi Algoritma Kriptografi Hibrida

Penelitian ini mengadopsi enkripsi hibrida yang menggabungkan AES (*Advanced Encryption Standard*) sebagai algoritma simetris dengan RSA (*Rivest–Shamir–Adleman*) sebagai algoritma asimetris. AES dipilih karena memiliki kinerja yang efisien dan telah teruji dalam berbagai studi [5] [6]. AES mampu mengenkripsi data dalam jumlah besar dengan cepat dan aman. Namun, distribusi kunci AES menjadi tantangan tersendiri, sehingga RSA digunakan untuk mengamankan kunci AES tersebut [7]-[10]. Strategi ini telah direkomendasikan oleh penelitian-penelitian sebelumnya untuk meningkatkan keamanan tanpa mengorbankan efisiensi [7]-[10]. Dalam penerapan, data slip gaji akan dienkripsi terlebih dahulu menggunakan AES, kemudian kunci AES yang digunakan akan dienkripsi menggunakan kunci publik RSA penerima. Pada saat penerima ingin mendekripsi data, ia menggunakan kunci privat RSA untuk mendapatkan kembali kunci AES dan selanjutnya mendekripsi data gaji.

D. Integrasi Autentikasi Multi-Faktor (MFA) Berbasis TOTP

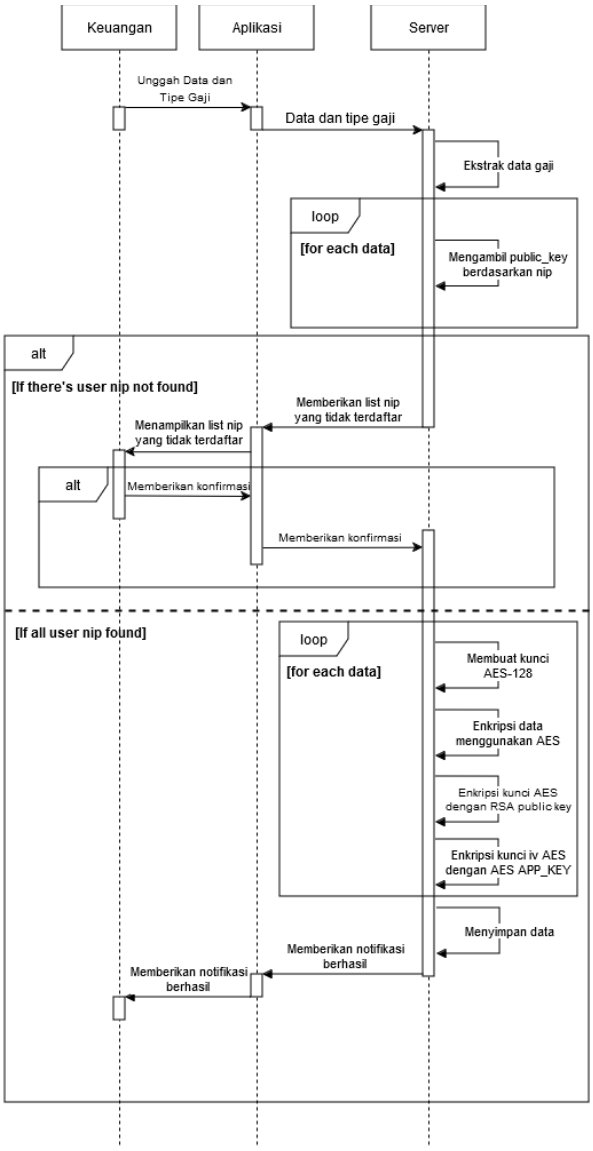
Untuk memperkuat mekanisme autentikasi pengguna, diterapkan metode MFA berbasis TOTP. Setiap kali pengguna melakukan aksi sensitif, seperti mengunduh slip gaji, sistem akan meminta kode OTP yang dihasilkan dari aplikasi autentikasi (misalnya *Google Authenticator*) [11] [12]. Pendekatan ini sesuai dengan praktik keamanan modern yang direkomendasikan untuk mengurangi risiko akses tidak sah dan pencurian kredensial. Penelitian terdahulu menunjukkan bahwa dengan menambahkan lapisan autentikasi berbasis waktu, sistem menjadi lebih tahan terhadap serangan *replay* dan pencurian *password* [11] [12].

Proses enkripsi data slip gaji pada sistem secara keseluruhan terdapat pada Gambar 3. Gambar tersebut merupakan diagram sekuens yang menggambarkan alur interaksi antara tiga entitas utama, yaitu Keuangan, Aplikasi, dan Server, saat proses unggah data slip gaji berlangsung. Diawali dengan Keuangan mengirimkan file yang berisi data slip gaji serta tipe gaji melalui Aplikasi, kemudian Aplikasi meneruskan data tersebut ke Server untuk diekstraksi dan diproses. Server akan memeriksa setiap entri data gaji untuk memastikan NIP pegawai terdaftar dalam sistem. Jika ditemukan NIP yang tidak dikenali, Server mengembalikan daftar NIP tersebut ke Aplikasi agar ditampilkan kepada Keuangan, yang dapat memutuskan untuk tetap melanjutkan pemrosesan data lain atau menghentikannya. Apabila diputuskan untuk melanjutkan, Server akan mengenkripsi data gaji menggunakan algoritma AES, lalu mengenkripsi kunci AES tersebut dengan kunci publik RSA milik pegawai, serta mengamankan IV (*Initialization Vector*) dengan *APP_KEY*. Data yang telah dienkripsi dan diamankan kemudian disimpan dalam basis data. Setelah seluruh proses selesai, Server memberikan notifikasi keberhasilan ke Aplikasi, yang kemudian menginformasikannya kepada Keuangan. Dengan demikian, diagram ini menampilkan mekanisme keamanan dan verifikasi data yang terintegrasi, memastikan hanya data gaji untuk NIP yang valid dan terdaftar yang diproses, serta seluruh proses dijalankan dengan langkah-langkah enkripsi hibrida untuk menjaga kerahasiaan dan integritas informasi.

E. Desain Basis Data dan Integrasi API

Struktur basis data dirancang dengan mempertimbangkan kebutuhan penyimpanan data sensitif, pengelolaan kunci, serta relasi antara pengguna, peran, dan izin [1] [2]. Pengguna yang telah terdaftar akan memiliki sepasang kunci RSA (*public* dan *private key*) yang disimpan

secara terenkripsi. Data slip gaji yang diunggah akan disimpan dalam bentuk terenkripsi menggunakan AES, dan kunci AES-nya diamankan menggunakan RSA, sesuai rekomendasi studi yang menekankan pentingnya pengamanan data sensitif dalam lingkungan terdistribusi [1] [2]. Selain itu, untuk mendukung integrasi dengan sistem eksternal, API dibangun dan diamankan dengan autentikasi berbasis API Key. API Key di-*hash* dan disimpan dengan aman, sedangkan hak akses (*permissions*) dikendalikan melalui kontrol *granular* berbasis *role* [9] [10].



Gambar 3. Proses Enkripsi Data Slip Gaji

F. Pengujian dan Evaluasi

Tahap pengujian meliputi pengukuran waktu enkripsi/dekripsi, konsumsi sumber daya komputasi, serta uji beban dalam skenario jumlah pesan yang berbeda [3] [4]. Metode evaluasi ini mengacu pada penelitian sebelumnya yang menekankan pengujian performa untuk memastikan sistem tetap responsif dan aman [3] [4]. Pengukuran dilakukan menggunakan serangkaian skenario terkontrol, di mana efisiensi enkripsi AES, kompleksitas dekripsi RSA, serta performa MFA TOTP dievaluasi. Dengan pendekatan ini, hasil pengujian diharapkan mampu menunjukkan bahwa penggunaan enkripsi hibrida dan TOTP dapat diimplementasikan tanpa menghambat kinerja sistem secara signifikan [5]-[8].

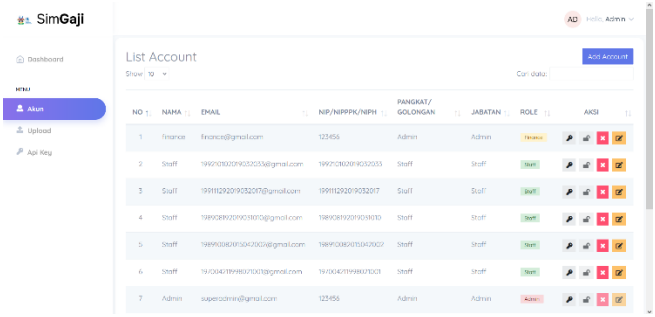
G. Validasi dan Siklus Iteratif

Setelah implementasi awal, sistem akan divalidasi oleh pihak-pihak terkait, seperti pengelola keuangan dan tim TIK, untuk memastikan bahwa proses distribusi slip gaji berjalan sesuai kebutuhan dan standar keamanan yang ditetapkan. Jika ditemukan kekurangan atau celah keamanan, sistem akan disempurnakan kembali dalam sprint selanjutnya, sejalan dengan prinsip pengembangan iteratif dan adaptif yang dianjurkan dalam Scrum [13] [16]. Siklus ini akan terus berlanjut hingga sistem mencapai kondisi yang stabil, aman, dan dapat diandalkan, sebagaimana diharapkan dalam penelitian ini.

III. HASIL DAN PEMBAHASAN

Gambar Gambar 4 menunjukkan tampilan antarmuka dari sistem pengelolaan akun pengguna yang dihasilkan melalui implementasi *framework Laravel* dalam penelitian ini. Pada halaman tersebut, terlihat daftar akun yang terdaftar dalam sistem, beserta informasi penting seperti nama, email, NIP/NIPPPK/NIPH, pangkat/golongan, jabatan, dan peran (role) masing-masing pengguna. Ikon-ikon pada kolom "Aksi" menunjukkan fungsionalitas yang dapat dilakukan administrator, misalnya mengubah data pengguna, menghapus akun, menonaktifkan/menonaktifkan autentikasi dua faktor (TOTP), atau mereset kata sandi.

Seluruh elemen yang ditampilkan mulai dari pengambilan data, pengurutan (*sort*), pencarian (*search*), penambahan akun (*Add Account*), hingga pengaturan hak akses diimplementasikan dari *Laravel*. *Framework* ini memberikan struktur yang semacam *Model-View-Controller*, pengelolaan *database* yang terintegrasi (melalui *Eloquent* ORM). Kemudahan dalam penerapan logika bisnis dan kebijakan keamanan juga diatur pada teknologi ini. Dengan demikian, implementasi Laravel dalam penelitian ini mempermudah pengembangan antarmuka administrasi, memungkinkan peneliti untuk memfokuskan pada integrasi fitur keamanan (enkripsi hibrida, TOTP) dan penerapan metodologi *Scrum*. Dari hal tersebut maka keseluruhan proses pengelolaan akun dan distribusi slip gaji dapat berjalan secara efisien, aman, dan adaptif.



Gambar 4. Implementasi SIM Gaji dengan Laravel

Setelah menerapkan metode yang telah dirancang, pengujian sistem dilakukan untuk mengevaluasi kinerja enkripsi hibrida AES-RSA, integrasi MFA berbasis TOTP, serta efektivitas metodologi pengembangan perangkat lunak yang digunakan. Pengujian difokuskan pada tiga aspek utama: (1) Kinerja kriptografi (waktu enkripsi/dekripsi,

konsumsi sumber daya komputasi), (2) Keamanan akses (MFA TOTP), serta (3) Evaluasi proses pengembangan menggunakan Scrum dan framework Laravel. Pengujian kinerja kriptografi dilakukan dengan mengukur waktu eksekusi enkripsi AES-128 untuk data slip gaji berukuran rata-rata 10 KB, serta waktu dekripsi kunci AES menggunakan RSA. Berikut adalah hasil rata-rata dari 100 kali percobaan.

Data pada Tabel 1 menunjukkan bahwa enkripsi AES-128 sangat efisien, sementara dekripsi RSA memang membutuhkan waktu dan sumber daya memori (RAM) lebih besar. Meski demikian, penggunaan RSA hanya terbatas pada proses dekripsi kunci AES, bukan data secara keseluruhan, sehingga dampaknya terhadap kinerja total sistem relatif kecil.

Tabel 1. Pengujian Eksekusi per Penggunaan RAM

Metode	Rata-rata Waktu Eksekusi	Deviasi Standar	Penggunaan RAM (KB)
Enkripsi AES-128	0,15 ms per slip	±0,02 ms	3,4 KB
Dekripsi Kunci AES (RSA)	5 ms per operasi	±0,5 ms	19,9 KB

Untuk aspek keamanan akses, pengujian dilakukan dengan melakukan 50 kali simulasi serangan *brute force* pada sistem yang telah mengaktifkan TOTP sebagai faktor autentikasi kedua.

Tabel 2. Pengujian Brute Force

Skenario	Jumlah Percobaan Akses Tidak Sah	Tingkat Keberhasilan Serangan
Tanpa TOTP (hanya *password*)	50 kali percobaan	12% (6 upaya berhasil)
Dengan TOTP aktif (*password* + OTP)	50 kali percobaan	0% (tidak ada yang berhasil)

Dari tabel tersebut dapat disimpulkan bahwa penerapan TOTP berhasil menurunkan tingkat keberhasilan akses tidak sah dari 12% menjadi 0%. Hal ini memperkuat klaim bahwa MFA berbasis TOTP secara signifikan meningkatkan keamanan akses ke data sensitif.

A. Kinerja Kriptografi Hibrida AES-RSA

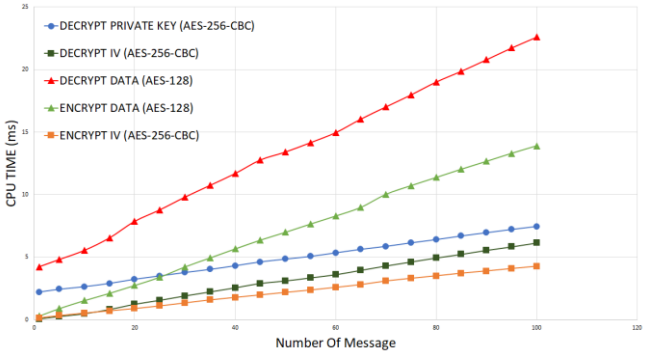
Hasil pengujian pada Tabel 1 menunjukkan proses enkripsi data slip gaji menggunakan AES dapat berjalan dengan sangat efisien. Waktu eksekusi enkripsi rata-rata berada pada skala milidetik per transaksi untuk ukuran data slip gaji yang relatif kecil. Hal ini konsisten dengan temuan dalam literatur yang menyatakan bahwa AES memiliki kecepatan tinggi dan efisiensi yang baik [5] [6]. Ketika jumlah pesan meningkat, waktu enkripsi AES bertambah secara hampir linear, namun tetap dalam batas yang dapat diterima untuk keperluan operasional.

Proses dekripsi kunci AES menggunakan RSA memerlukan waktu eksekusi yang lebih besar dibandingkan enkripsi. Hal ini sejalan dengan karakteristik RSA yang secara matematis lebih kompleks pada tahap dekripsi [7]-[10]. Meskipun demikian, karena RSA hanya digunakan untuk mengenkripsi dan mendekripsi kunci AES (bukan data slip gaji secara keseluruhan), overhead ini tidak menjadi kendala signifikan pada skala sistem yang telah diuji. Dengan demikian, pendekatan hibrida memanfaatkan keunggulan AES dalam hal kecepatan untuk enkripsi data, sementara RSA memastikan keamanan distribusi kunci, sebagaimana direkomendasikan pada penelitian sebelumnya [8] [9].

Penggunaan super-enkripsi RSA-AES-128 pada dokumen tertentu juga dapat meningkatkan keamanan, terutama dalam skenario yang memerlukan perlindungan berlapis [10]. Secara keseluruhan, hasil menunjukkan bahwa pendekatan enkripsi hibrida ini berhasil mencapai keseimbangan antara keamanan dan efisiensi, mendukung rekomendasi sebelumnya di bidang komputasi awan dan integrasi keamanan data sensitif [3] [4].

B. Integrasi Autentikasi Multi-Faktor (MFA) Berbasis TOTP

Hasil yang ditunjukkan pada Tabel 2 yang mana penerapan TOTP berhasil menambah lapisan keamanan terhadap akses data sensitif. Setiap kali pengguna hendak mengunduh slip gaji atau melakukan aksi sensitif lainnya, sistem meminta kode OTP yang dihasilkan secara dinamis oleh aplikasi autentikator. Pengujian menunjukkan bahwa pengguna yang gagal memasukkan kode TOTP dengan benar tidak dapat melanjutkan proses, sesuai tujuan untuk mencegah akses tidak sah [11] [12].



Gambar 5. Pengujian Enkripsi AES

Pada Gambar 5 mengindikasikan bahwa proses dekripsi membutuhkan *computational cost* yang lebih tinggi dibandingkan dengan proses enkripsi untuk jumlah pesan yang sama. Penggunaan *computational cost* yang lebih tinggi pada proses dekripsi disebabkan oleh kompleksitas proses dekripsi yang melibatkan beberapa tahapan tambahan, seperti pengolahan *private key* dan *IV*, yang membutuhkan lebih banyak komputasi dibandingkan dengan enkripsi yang lebih langsung.

Hasil ini konsisten dengan penelitian sebelumnya yang menekankan pentingnya MFA dalam memperkuat keamanan sistem yang menangani data sensitif. Dengan menambahkan faktor berbasis waktu, kemungkinan serangan replay atau penggunaan ulang kredensial lama dapat diminimalisir [11]. Hal ini membuktikan bahwa integrasi TOTP pada sistem distribusi slip gaji meningkatkan tingkat perlindungan, sejalan dengan tren keamanan modern.

C. Evaluasi Metodologi Pengembangan dan Framework yang Digunakan

Proses pengembangan sistem menggunakan Scrum dan kerangka kerja Laravel memberikan hasil yang memuaskan

dalam hal adaptabilitas dan kemudahan pengelolaan kode sumber. Selama beberapa sprint, tim pengembang dapat dengan cepat menyesuaikan fitur keamanan maupun fungsionalitas sistem berdasarkan umpan balik pengguna [13] [16]. Penggunaan Laravel memudahkan implementasi fitur-fitur inti, seperti routing, manajemen basis data, dan pembuatan API. Studi kasus sebelumnya telah menunjukkan efektivitas Laravel untuk pengembangan aplikasi berskala kecil hingga menengah [14] [15].

Pada akhirnya, integrasi metodologi pengembangan yang iteratif dan adaptif ini mendukung prinsip continuous improvement, sehingga setiap perbaikan yang diperlukan—baik dari sisi keamanan, kinerja, maupun user experience—dapat diimplementasikan secara cepat. Kesesuaian hasil ini dengan temuan dalam studi literatur menegaskan bahwa pendekatan Agile melalui Scrum, didukung oleh framework modern, menjadi strategi yang efektif dalam menciptakan sistem informasi yang responsif dan mudah dipelihara [13] [15] [16].

Hasil pengujian sistem distribusi slip gaji yang telah diimplementasikan menunjukkan bahwa penggunaan enkripsi hibrida AES-RSA efektif untuk mengamankan data slip gaji tanpa berdampak signifikan pada kinerja sistem. Integrasi MFA berbasis TOTP berhasil meningkatkan tingkat keamanan akses, sehingga hanya pengguna yang terverifikasi yang dapat mengunduh data sensitif. Selain itu, penerapan Scrum dan Laravel dalam proses pengembangan terbukti mendukung adaptabilitas serta efisiensi pengembangan.

Temuan ini sejalan dengan penelitian-penelitian terdahulu yang menekankan pentingnya pendekatan hibrida dalam enkripsi [7]-[10], peran MFA dalam keamanan siber [11] [12], serta manfaat metode Agile dalam pengembangan perangkat lunak [13] [16] [17]. Dengan demikian, penelitian ini diharapkan dapat menjadi acuan bagi institusi lain dalam mengelola distribusi data sensitif, seperti slip gaji, secara aman, efisien, dan fleksibel.

IV. KESIMPULAN

Pada Penelitian ini telah berhasil dirancang dan diimplementasikan sistem distribusi slip gaji digital yang mengintegrasikan enkripsi hibrida (AES-RSA), autentikasi dua faktor berbasis TOTP, serta metodologi *Scrum* dengan dukungan *Laravel*. Integrasi ini dimuat sehingga tercapai inovasi dalam mengamankan data sensitif tanpa mengorbankan kinerja sistem. Pendekatan ini memberikan kontribusi nyata: AES meningkatkan kecepatan enkripsi/dekripsi data, RSA menjaga keamanan kunci AES, dan TOTP mengurangi risiko akses tidak sah, sementara *Scrum* dan teknologi Laravel mempermudah pengembangan yang adaptif dan terukur. Dampak positifnya adalah proses distribusi slip gaji menjadi efisien, aman, dan dapat diandalkan, meningkatkan kenyamanan bagi institusi dan karyawan yang bergantung pada informasi penggajian. Untuk memaksimalkan manfaat ini, penelitian lanjutan disarankan mencakup pengujian pada beban lebih besar untuk memastikan skalabilitas, penambahan fitur audit keamanan agar aktivitas dapat dilacak dan dianalisis secara detail, serta eksplorasi skenario yang lebih kompleks guna menghadapi tantangan keamanan data yang semakin canggih di masa depan[1]-[4].

UCAPAN TERIMA KASIH

Ucapan terima kasih saya sampaikan kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Institut Teknologi Kalimantan (ITK) atas dukungan dan fasilitasi yang telah diberikan selama proses penelitian ini berlangsung. Bantuan yang mencakup akses sumber daya, pendampingan, serta kesempatan untuk mengembangkan riset di lingkungan akademis yang kondusif sangat berharga dalam mewujudkan tujuan serta hasil penelitian ini. Semoga dapat terus berlanjut dan memberikan kontribusi yang positif bagi pengembangan ilmu pengetahuan dan teknologi di masa mendatang.

REFFERENSI

[1] N. Afni, R. Pakpahan, and A. Rezky Jumarah, "Rancang Bangun Sistem Informasi Penggajian Dengan Implementasi Metode Waterfall," Jurnal Ilmu Komputer, vol. VII, Dec. 2019.

[2] M. A. Hasan and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," 2022.

[3] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," International Journal of Artificial Intelligence Research, vol. 4, no. 1, 2020, doi: 10.29099/ijair.v4i1.154.

[4] [4] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric Encryption Algorithms: Review and Evaluation study," International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 2, 2020.

[5] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," IEEE Access, vol. 9, pp. 155949–155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[6] R. Akter, M. A. R. Khan, F. Rahman, S. J. Soheli, and N. J. Suha, "RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing," International Journal of Computational and Applied Mathematics & Computer Science, vol. 3, pp. 60–71, 2023, doi: 10.37394/232028.2023.3.8.

[7] S. Deepika, V. D. L. Rajeswari, R. Yamini Varma, S. Ramya, and M. Y. Vineela Sravya, "Secure data transmission using hybrid cryptography," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 8, no. 8, 2021.

[8] V. Mahesh, B. Batta, and L. K. Suresh Kumar, "RSA-AES Hybrid Encryption: Combining The Strengths Of Two Powerful Algorithms For Enhanced Security," International Journal of Research and Analytical Reviews, 2023.

[9] K. Jaspin, S. Selvan, S. Sahana, and G. Thanmai, "Efficient and secure file transfer in cloud through double encryption using AES and RSA algorithm," in 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021, pp. 791–796, doi: 10.1109/ESCI50559.2021.9397005.

[10] F. Nuraeni, D. Kurniadi, N. Rahayu, and J. I. Komputer, "Implementation Of RSA And AES-128 Super Encryption On QR-Code Based Digital

Signature Schemes For Document Legalization," Jurnal Teknik Informatika (JUTIF), vol. 5, no. 3, pp. 675–684, 2024, doi: 10.52436/1.jutif.2024.5.3.1426.
[11] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," Digital Health, vol. 9, 2023.
[12] L. Lumburovska, J. Dobreva, S. Andonov, H. M. Trpcheska, and V. Dimitrova, "A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose?," 2023.
[13] H. Edison, X. Wang, and K. Conboy, "Comparing Methods for Large-Scale Agile Software Development: A Systematic Literature Review," IEEE Transactions on Software Engineering, vol. 48, no. 8, pp. 2709–2731, 2022, doi: 10.1109/TSE.2021.3069039.
[14] M. Amini, A. Rahmani, M. Abedi, M. Hosseini, M. Amini, M. Amini, and M. Gostar, "Mahamgostar.Com As A Case Study For Adoption Of Laravel Framework As The Best Programming Tools For Php Based Web Development For Small And Medium Enterprises," 2020. [Online]. Available: www.mahamgostar.com
[15] [Y. Wahyudin and D. N. Rahayu, "Analisis Metode Pengembangan Sistem Informasi Berbasis Website: A Literature Review," Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi, vol. 15, no. 3, pp. 26–40, 2020, doi: 10.35969/interkom.v15i3.74.
[16] A. C. Sassa, I. A. De Almeida, T. Nakagomi, F. Pereira, and M. S. De Oliveira, "Scrum: A Systematic Literature Review," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 14, no. 4, 2023.
[17] Z. Purnomo Prodi Sistem Informasi, J. Karim Prodi Sistem Informasi, B. Senung Prodi Sistem Informasi, dan S. Abdussamad, "Sistem Informasi Jasa Pemesanan Percetakan Berbasis Android," Jambura Journal of Electrical and Electronics Engineering, vol. 2, no. 2, hlm. 44–51, Jul 2020, doi: https://doi.org/10.37905/jjeee.v2i2.6006.