BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi telah mendorong munculnya tanda tangan elektronik *(e-signature)* sebagai komponen penting dalam proses verifikasi identitas digital, autentikasi dokumen, dan pelaksanaan transaksi. Melalui penggunaan *e-signature*, individu maupun organisasi dapat melakukan pengesahan dokumen tanpa memerlukan pertemuan tatap muka, sehingga meningkatkan efisiensi proses bisnis serta menekan biaya operasional [1].

Sebagai implementasi dari perkembangan tersebut, dikembangkan aplikasi E-Signing yang berfungsi memfasilitasi proses penandatanganan dokumen dan data secara *digital*. Aplikasi ini diintegrasikan dengan *Hardware Security Module (HSM)* untuk menjamin keamanan pengelolaan kunci kriptografi. HSM berperan dalam melindungi kunci privat, membatasi akses yang tidak sah, serta memastikan keaslian dan integritas tanda tangan elektronik yang dihasilkan.

Untuk memperkuat aspek keamanan dan akuntabilitas, aplikasi E-Signing dilengkapi dengan sistem *logging* yang mencatat seluruh aktivitas pengguna, mulai dari proses autentikasi hingga penandatanganan dokumen. Sistem *logging* merupakan komponen esensial dalam infrastruktur keamanan sistem informasi modern karena berfungsi membentuk *audit trail* yang merekam setiap aktivitas dan transaksi yang terjadi di dalam sistem. *Audit trail* menyediakan catatan aktivitas pengguna dan status sistem yang berguna untuk keperluan audit, forensik digital, serta pemeliharaan sistem, sekaligus memungkinkan penelusuran kembali terhadap kesalahan operasional maupun aktivitas yang bersifat mencurigakan [2]. Dengan adanya *audit trail*, auditor dapat menelusuri transaksi atau *event* secara menyeluruh sejak awal terjadinya hingga proses akhir [3, 4].

Dalam konteks bisnis dan teknologi informasi, *audit* memiliki peran strategis dalam menjamin transparansi dan akuntabilitas sistem. Keberadaan *audit trail* memungkinkan setiap perubahan data atau transaksi ditelusuri kembali ke sumbernya, sehingga memudahkan identifikasi kesalahan, penyimpangan, maupun tindakan yang tidak sesuai prosedur. Transparansi ini juga memungkinkan manajemen melakukan pemantauan dan pengendalian aktivitas sistem secara berkelanjutan, sehingga risiko kesalahan atau penyalahgunaan dapat segera

diidentifikasi dan ditindaklanjuti [4].

Secara regulatif, sistem informasi yang menggunakan tanda tangan elektronik diwajibkan menerapkan *audit trail* yang aman, dihasilkan secara *digital*, serta dilengkapi dengan *timestamp* untuk mencatat tanggal dan waktu setiap tindakan yang membuat, mengubah, atau menghapus catatan elektronik tanpa mengaburkan informasi yang telah tercatat sebelumnya. Selain itu, sistem harus memiliki mekanisme pemeriksaan kewenangan untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses sistem, memberikan tanda tangan elektronik, maupun melakukan perubahan data. Setiap tanda tangan elektronik juga harus bersifat unik bagi satu individu dan tidak dapat digunakan kembali atau dialihkan kepada pihak lain [5].

Data *log* atau *audit trail* yang dihasilkan sistem memiliki nilai penting sebagai pendukung keaslian barang bukti, khususnya dalam konteks forensik digital. Serupa dengan *black box* pada pesawat yang merekam setiap peristiwa selama penerbangan, *log* sistem mencatat seluruh kejadian yang terjadi di dalam sistem, termasuk aktivitas aplikasi dan interaksi jaringan. Setiap *event* menghasilkan data *log* yang merepresentasikan berbagai entitas kejadian, sehingga memungkinkan rekonstruksi kondisi dan keadaan sistem pada saat peristiwa tersebut terjadi [6]. Audit trail yang terkelola dengan baik juga berperan dalam mendukung keandalan bukti digital serta meningkatkan kepercayaan terhadap sistem informasi yang diaudit [7].

Oleh karena itu, perhatian khusus harus diberikan pada verifikasi integritas data serta perlindungan terhadap informasi sensitif. Aktivitas pencegahan kehilangan dan penyalahgunaan data merupakan bagian dari proses *audit* yang mencakup identifikasi kerentanan dan risiko, evaluasi kecukupan pengendalian keamanan, serta penilaian validitas perangkat keamanan dan mekanisme *audit*. Proses ini juga mencakup pemantauan berkelanjutan terhadap efektivitas pengendalian keamanan yang diterapkan [8].

Dengan adanya sistem pencatatan yang terstruktur dan aman, penggunaan tanda tangan elektronik tidak hanya meningkatkan efisiensi administrasi, tetapi juga memperkuat transparansi dan akuntabilitas dalam hubungan kerja. Melalui sistem *digital* yang terintegrasi, proses pembuatan, penyimpanan, serta pengawasan dokumen menjadi lebih sistematis dan mudah diaudit oleh pihak yang berwenang [9].

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari pelaksanaan kerja magang ini adalah untuk:

- Memberikan pengalaman langsung di dunia industri, khususnya dalam bidang teknologi informasi dan pengembangan perangkat lunak.
- Meningkatkan pemahaman dan keterampilan dalam pengembangan *software*, aplikasi, dan sistem.
- Memberikan kesempatan untuk terlibat dalam proyek-proyek yang relevan dengan industri.

Tujuan dari magang ini adalah untuk mengembangkan *logging system* untuk aplikasi *E-Signing*.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan magang berlangsung selama total 640 jam, dimulai pada 14 Juli 2025 hingga 7 November 2025. Kegiatan magang dilaksanakan secara *Work from Office* (WFO) di kantor yang beralamat di Jl. Bougenville II No.5 Blok B9, Jelupang, Serpong Utara, Kota Tangerang Selatan, Banten. Kegiatan dilakukan pada hari kerja, yaitu Senin hingga Jumat, dengan jam kerja yang ditetapkan dari pukul 09.00 hingga 18.00 WIB dan waktu istirahat menyesuaikan kebijakan perusahaan.

Setiap minggu diberi arahan dari *supervisor* serta melakukan sesi konsultasi terkait perkembangan pekerjaan yang sedang dikerjakan. Revisi atau penyempurnaan hasil kerja dilakukan apabila terdapat *feedback* dari *supervisor* maupun *PIC* lain yang terkait.