BAB 1
PENDAHULUAN

1.1 Latar Belakang

Diera gempuran teknologi informasi ilmu pengetahuan berkembang dengan pesat. Hal ini dipengaruhi dengan adanya percepatan pertukaran informasi yang terjadi saat ini. Salah satu elemen yang mempengaruhi percepatan informasi ini adalah perguruan tinggi. Perguruan tinggi berupa lembaga pendidikan memiliki peran dan tugasnya dalam penelitian dan juga pengembangan terhadap teknologi informasi saat ini [1]. Perguruan tinggi ini mencakup berbagai bentuk lembaga akademi seperti politeknik, sekolah tinggi, institusi, dan juga universitas. Dimana setiap perguruan tinggi diatur dalam undang-undang mentri pendidikan yang meneyebutkan setiap perguruan tinggi memiliki kewajiban dalam menyelenggarakan pendidikan, penelitian, dan juga pengabdian kepada masyarakat sebagaimana dalam peraturan Mentri Pendidikan dan Kebudayaan No. 3 Tahun 2020 tentang Standar Nasional Pendidikan Tinggi [2].

Universitas Komputer Indonesia atau yang dikenal dengan UNIKOM merupakan universitas swasta yang berlokasi di Jl. Dipati Ukur No.112-116, Lebak Gede, Coblong, Bandung, Provinsi Jawa Barat. Unikom berperan dalam mewujudkan pendidikan dan aktif dalam pengembangan ilmu pengetahuan dan teknologi. Divisi Penelitan, Pengabdian, dan Pemberdayaan Masyarakat atau yang disingkat dengan DP3M UNIKOM bergerak membantu para dosen dalam melakukan pengabdian kepada masyarakat seperti pendidikan kepada masyarakat, pelayanan kepada masyarakat dan juga pengembangan dan penerapan hasil penelitian. Dimana dalam laporan pengabdian tersebut diperlukan tanda tangan pada lembar pengajuan dari Kaprodi, Dekan dan ketua Divisi yang kadang berhalangan hadir di kampus. Akibatnya terjadinya keterlambatan, dan penundaan waktu bagi dosen yang sedang melaksanakan pengabdian dan pemberdayaan masyarakat tersebut.

Permasalahan tersebut dapat diselesaikan dengan mengirimkan lembar yang akan ditanda tangan menggunakan jejaring sosial dalam bentuk digital baik dalam bentuk word ataupun pdf lalu dicetak dan ditanda tangan dan dikirim kembali dalam bentuk digital. Selain cara ini dinilai kurang efektif juga diragukan keamanan berkas yang dikirim secara digital tersebut. Dikarenakan berkas yang dikirimkan dalam bentuk *plaintext* ini beresiko apabila ada pihak lain yang berhasil meretas dan merubah informasi, melakukan pemalsuan dan pembajakan pada dokumen digital tersebut [3].

Dari permasalahan tersebut diperlukan metode yang digunakan untuk melakukan tanda tangan secara online, salah satunya adalah *digital signature*. *Digital signature* merupakan salah satu metode keamanan berkas digital yang menerapkan teknologi kriptografi. Dimana cara kerjanya dokumen digital dirubah menjadi *message digest*, sebuah fungsi keluaran dari *hash* berbentuk simbol dan angka matematis yang kemudian dienkripsi menggunakan algoritma kriptografi *asimetris*, hasil dari enkripsi tersebutlah yang menjadi tanda tangan dari dokumen tersebut [4]. *Elliptic Curve Digital Signature Algorithm* (ECDSA) merupakan pengembangan dari *Digital Signature Algorithm* (DSA) yang menggunakan *elliptic curve* untuk menentukan *key*. Seperti DSA, ECDSA terdiri dari tiga tahap yaitu menentukan *key*, tahap penanda tanganan, dan tahap verifikasi [5].

Dari poin-poin permasalahan yang telah diuraikan diatas maka dibuatlah penelitian ini, di harapkan dapat menjadi solusi pemecah permasalahan yang telah diuraikan. Peneliti berinisiatif membangun sebuah sistem yang memanfaatkan teknologi *digital signature* dengan menggunakan metode enkripsi ECDSA (*Elliptic Curve Digital Signature Algorithm*) sebagai enkripsi keamanan sistemnya yang bertujuan untuk membantu menangani permasalahan tersebut.

1.2 Identifikasi Masalah

Dari latar belakang masalah tersebut maka masalah yang didapat identifikasi sebagai berikut ini :

1. Diperlukannya sistem yang dapat melakukan tandatangan digital pada lembar pengesahan pengabdian.

2. Kurangnya keamanan dalam melakukan tandatangan menggunakan gambar tandatagan basah yang di tempelkan pada berkas secara digital.

1.3 Maksud dan Tujuan

Adapun maksud dan tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1.3.1 Maksud

Dari latar belakang diatas maka maksud dari penelitian ini adalah untuk membangun prototipe aplikasi yang dapat melakukan tanda tangan digital dan juga meningkatkan keamanan berkas yang ditanda tangani tersebut dengan teknologi digital signature menggunakan metode enkripsi ECDSA.

1.3.2 Tujuan

Adapun tujuan yang hendak dicapai dari penelitian ini adalah sebagai berikut ini:

1. Mengimplementasi tandatangan digital Pada lembar pengesahan pengabdian.
2. Mengamankan tandatangan digital lembar pengesahan pengabdian.

1.4 Batasan Masalah

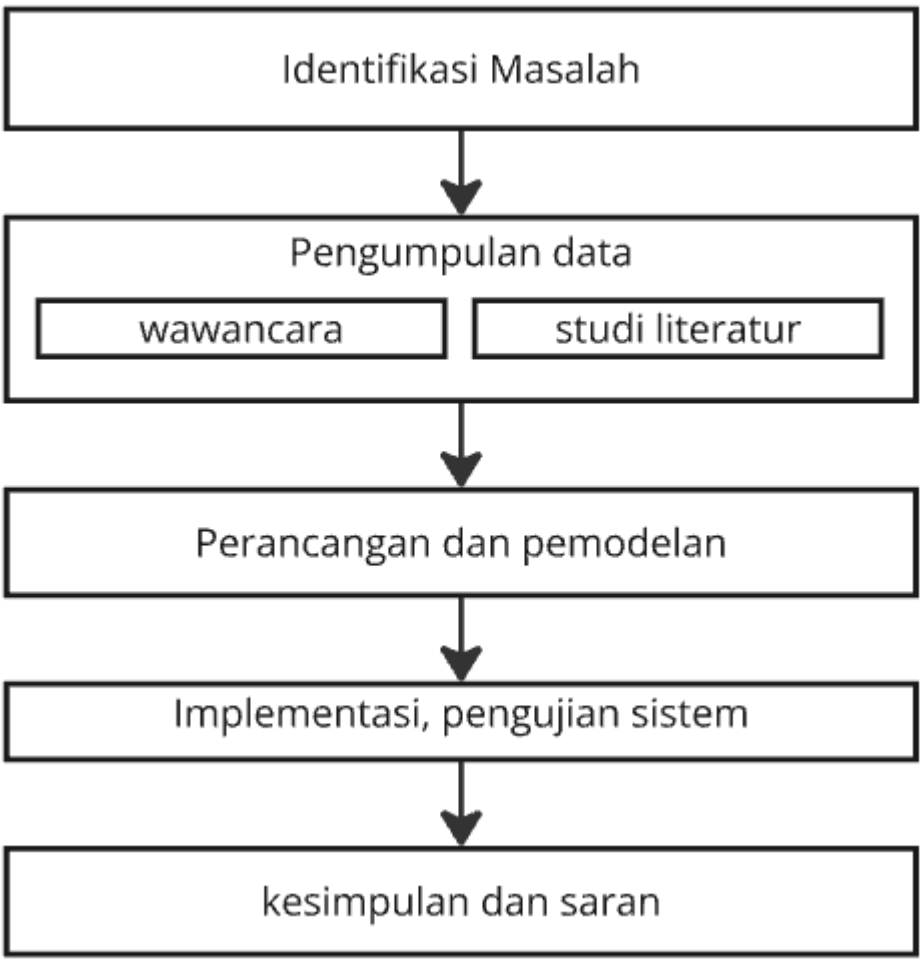
Agar penelitian terfokus dan tidak meluas dari pembahasan maka dibuatlah batasan-batasan masalah agar tujuan dari penelitian ini dapat dicapai. Berikut batasan masalah yang ada pada sistem ini:

1. Tempat penelitian ini berada pada di Divisi SIM DP3M.
2. Data yang akan diolah sistem adalah mengenai lembar pengajuan.
3. Bentuk tandatangan yang akan digunakan pada lembar adalah qrcode.
4. Lembar pengesahan yang akan digunakan berupa format pdf.
5. Pengguna sistem adalah Dosen, Kaprodi, Dekan dan juga Ketua Divisi P2M.

6. Bahasa pemograman yang digunakan adalah PHP dengan Mysql sebagai databasenya.

1.5 Metodelogi Penelitian

Metodologi penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, dimana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Metodologi penelitian yang digunakan adalah metode analisis deskriptif. Metode analisis deskriptif merupakan metode yang menggambarkan fakta-fakta dan informasi dalam situasi atau kejadian sekarang secara sistematis, faktual dan akurat [6].



Gambar 1. 1 Metode Penelitian

Berikut adalah penjelasan tahapan-tahapan yang digambarkan pada gambar 1.1 Metode penelitian :

1) Identifikasi Masalah, Melakukan identifikasi masalah yang terjadi di Divisi SIM Penelitian Pengabdian dan Pemberdayaan Masyarakat Unikom dengan cara observasi atau peninjauan secara langsung untuk melihat permasalahan yang terjadi.
2) Pengumpulan data, Pengumpulan data dilakukan dengan cara studi literatur dan juga melalukan wawancara tanya jawab dengan pihak Divisi SIM DP3M Unikom secara langsung**.**
3) Perancangan dan pemodelan, Pada tahap ini dilakukan analisis sistem dan juga perancangan sistem berdasarkan data dan juga masalah yang telah ditinjau sebelumnya.
4) Implementasi sistem dan pengujian sistem, Ditahap ini diawali dengan implementasi sistem berupa penulisan kode dengan rancang dan model yang telah ditentukan pada tahap sebelumnya. Dari hasil sementara implementasi dilakukan pengujian sistem dengan menggunakan prosedur black box hasil sementara dari pengujian ini dijadikan sebagai bahan evaluasi untuk memenuhi tujuan dari penelitian ini.
5) Kesimpulan dan saran, Pada tahap ini akan melakukan penarikan kesimpulan dari hasil pengujian sistem yang telah dibangun dengan mengacu dari tujuan penelitian yang ingin dicapai. Penelitian akan dikatakan berhasil apabila kesimpulan memenuhi tujuan penelitian. Tidak semua penelitian bisa memenuhi seluruh dari tujuan dari penelitian yang dilakukan oleh karena itu dibutuhkan saran yang akan menjadi patok pengembangan penelitian dimasa yang akan datang.

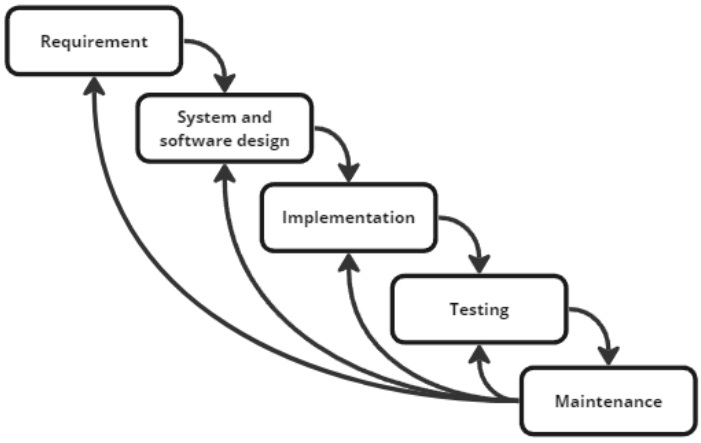
1.5.1 Metode Pengumpulan Data

Untuk melengkapi penelitian ini diperlukan data yang dapat mendukung permasalahan yang terjadi. Adapun metode yang dilakukan untuk mengumpulkan data adalah sebagai berikut:

1. Studi Literatur Mempelajari dasar teori dari berbagai literatur mengenai segala hal yang dibutuhkan untuk penelitian. Pencarian berupa referensi dari internet, buku, jurnal ilmiah, dapat berupa artikel, tutorial, dan bahasan dalam forum yang berkaitan dengan penelitian ini.
2. Wawancara Pengumpulan data dengan cara tanya jawab langsung dengan Divisi SIM DP3M unikom secara langsung.

1.5.2 Metode Pengembangan Perangkat Lunak

Metode pembangunan perangkat lunak atau SDLC (*Software Development Life Cycle*) yang akan digunakan dalam penelitian ini adalah *waterfall*. Dimana model ini dilakukan dengan pendekatan yang sistematis, mulai dari tahap kebutuhan sistem lalu menuju ke tahap analisis. Berikut ini adalah gambaran dari siklus model waterfall, dapat diamati pada Gambar 1.2 Model *Waterfall*.



Gambar 1. 2 Model *Waterfall*

Dimana tahap-tahapan metode *waterfall* diatas dideskripsikan di bawah ini [7]:

a. Requirement

Requiremment ini meliputi dari tahap wawancara dengan beberapa narasumber lalu diikuti dengan penentuan identifikasi masalah yang ditemukan, hingga analisis kebutuhan pengguna dan kebutuhan perangkat lunak.

b. System and Software Design

Di tahap ini penulisan dan pembuatan *design* dari aplikasi yang akan dibangun didokumentasikan kedalam bentuk yang lebih sistematis dengan pemodelan *Unified Modelling Languange* (UML). Di tahap ini juga dilakukan perancangan design antarmuka dari aplikasi yang akan dibangun.

c. Implementasi

Implementasi adalah tahap pembangunan aplikasi yang telah didesign pada tahap sebelumnya, dengan menggunakan software, bahasa pemograman dan juga algoritma yang sesuai dengan penelitian ini.

d. Testing

Setelah melalui tahap perancangan dan implementasi, aplikasi akan melalukan tahap *testing* untuk menguji kembali apakah aplikasi telah memenuhi kebutuhan yang diperlukan oleh pengguna atau belum.

e. Maintenance

Setelah tahapan *testing* dilakukan, kemudian dilakukan tahap *maintenance*. Tahap *maintenance* merupakan tahap perawatan aplikasi jika pada tahap *testing* ditemukan ketidaksesuaian dalam aplikasi.

1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini telah disusun untuk memberikan gambaran tentang penelitian yang akan dilakukan. Sistem penulisan dalam penelitian ini adalah:

BAB 1 PENDAHULUAN

Bab 1 menjelaskan latar belakang masalah, merumuskan inti masalah, menemukan solusi untuk masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab 2 membahas tentang teori-teori yang berhubungan dengan topik skripsi yang dibangun. Diantara teori yang dibahas adalah teori Digital signature, webiste, codeigniter, ECDSA, dan surat, serta teknologi yang digunakan dan beberapa teori pendukung lainnya.

BAB 3 ANALISIS DAN PERANCANGAN

Bab 3 menjelaskan tentang analisis dan Perancangan Sistem. Analisis meliputi analisis masalah, analisis spesifikasi kebutuhan perangkat lunak, analisis kebutuhan fungsional dan analisis kebutuhan non-fungsional, perancangan sistem, perancangan struktur menu, hingga desain tampilan antarmuka aplikasi yang akan dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab 4 membahas implementasi dari sistem yang akan dibangun dengan mengikuti perancangan pada bab sebelumnya. Setelah implementasi pada bab ini juga dilakukan pengujian perangkat lunak kepada narasumber wawancara sebelumnya dengan menggunakan metode pengujian *blackbox*.

BAB 5 KESIMPULAN DAN SARAN

Pada bab 5 ini berisi kesimpulan dari penelitian Pembangunan Digital Signature Di Universitas Komputer Indonesia menggunakan Metode ECDSA Pada Sistem SIM DP3M dengan hasil nilai tercapainya maksud dan tujuan pada penelitian ini.