BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan berjalannya modernisasi, tingkat risiko kejahatan pun akan semakin meningkat. Kondisi ini mengharuskan beberapa bahkan semua sistem berubah dari sistem konvensional menjadi digital secara berangsur dan signifikan. Hal kecil yang sering menjadi korban dari kejahatan ini adalah dokumentasi. Kejahatan pada dokumentasi biasanya adalah pemalsuan dokumen yang dapat merugikan korban, contohnya seperti tanda tangan yang ditiru atau dipalsukan dengan tujuan ingin mengambil hak dari korban untuk kepentingan pelaku. Setidaknya terdapat 151.750 kasus pelanggaran dengan kata kunci "Pemalsuan Dokumen" sejak tahun 2019 [1].

Pada tahun 2014 terjadi pemalsuan dokumen berupa surat izin mengemudi yang dapat menimbulkan kerugian, dan bahkan dapat berdampak kepada keselamatan pengguna lalu lintas [2]. Contoh kedua pelanggaran dokumentasi dilakukan oleh Untung Wiyono, mantan bupati Sragen, menggunakan ijazah Sekolah Menengah Atas (SMA) palsu saat mencalonkan diri sebagai bakal calon Bupati Sragen dalam Pemilihan Kepala Daerah (Pilkada) 2000-2006. Untung menggunakan ijazah SMA Sembada tahun 1971 bernomor seri LAA 001054 yang ternyata milik Ratna Hidayat dari SMA Negeri 6 Jakarta [3]. Masalah ini juga dapat disebabkan penggunaan dari bentuk fisik dari dokumen yang keamanannya sudah sangat berisiko.

Tidak hanya karena faktor keamanan, penggunaan bentuk fisik ini juga mulai dikurangi dengan kampanye ramah lingkungan dan efisiensi yang diberikan

oleh teknologi saat ini. Program atau sistem yang mengganti dari bentuk fisik kertas menjadi *paperless office* seperti tata naskah dinas elektronik yang sudah digunakan di beberapa internal instansi atau perusahaan. Bentuk *paperless office* ini memiliki beberapa perubahan sistem keamanan namun dengan konsep yang sama seperti dokumen bentuk fisik atau kertas.

Tanda tangan sudah jadi tanda legalitas dalam dokumen dengan tingkat risiko yang kecil sebelum jaman secanggih sekarang. Salah satu fungsi tanda tangan pada sebuah dokumen yaitu sebagai tanda bahwa dokumen telah dibaca dan disetujui oleh penanda tangan [4]. Tanda tangan ini membutuhkan kejelian dan kepercayaan dari pihak yang menerima dokumen tersebut, dengan kata lain jika penerima tidak meyakini dokumen itu benar-benar dikeluarkan oleh pihak yang seharusnya, maka fungsi tanda tangan sebagai legalitas ini sudah tidak relevan lagi.

Dengan teknologi seperti sekarang, sistem tanda tangan konvensional ini sudah sangat mudah untuk ditiru atau dipalsukan, sehingga tanda tangan saja dirasa tidak cukup untuk memenuhi sifat otentik dokumen. Masalah ini membutuhkan sistem yang dapat menjamin dokumen dengan tanda yang unik yaitu tanda yang hanya dimiliki oleh satu dokumen saja. Sehingga jika tanda tersebut disalin, tanda tidak akan lolos dalam identifikasi atau dinyatakan Dokumen palsu. Penambahan kriptografi dengan fungsi *hash* agar atribut yang menjadi identitas dokumen dapat tersimpan secara unik menjadi *message digest* dan tidak bisa dikembalikan ke dalam *plaintext* seperti semula. Setelah menjadi *message digest*, pesan akan degenerat menjadi *Qrcode*.

Berdasarkan masalah pelanggaran dokumen tersebut, tugas akhir ini yang berjudul “Sistem Penjamin Integritas untuk Keamanan Dokumen Menggunakan

Algoritma *Keccak* dan *Quick Response Code*" diajukan untuk membantu mengidentifikasi kebenaran dokumen.

1.2 Perumusan Masalah

Tanda tangan dapat digunakan berulang-ulang sebagai identitas dari pemilik yang bersifat unik untuk pemiliknya bukan terhadap dokumen, sehingga pemilik tidak dapat menyangkal jika terjadi kejahatan dokumentasi. Berdasarkan pada latar belakang tersebut, dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana cara menjaga integritas dokumen dengan Algoritma *Keccak*?
2. Bagaimana cara memberi tanda khusus untuk masing-masing dokumen?
3. Bagaimana cara cepat untuk mengetahui kebenaran dokumen?

1.3 Batasan Masalah

Agar penelitian dapat terarah dan sesuai dengan tujuan yang diinginkan, maka batasan dari rancangan sistem yang dibuat sebagai berikut:

1. Sistem hanya dapat memproses dokumen dalam bentuk PDF,
2. Sistem hanya berlaku untuk dokumen yang sudah final, yaitu dokumen sudah disahkan dan tidak mendapatkan perubahan lagi,
3. Sistem tidak mengacu terhadap proses bisnis pengajuan dokumen pihak mana pun.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu membuat sistem penjamin yang dapat membantu mengidentifikasi kebenaran dokumen bernama "Penjamin Integritas Dokumen" dengan menggunakan algoritma *keccak* pada metode *Hash Message Authentication Code* (HMAC) untuk mengacak gabungan konten dokumen dan

dilakukan penambahan data dalam bentuk *Qrcode* yang berfungsi sebagai penjamin kebenaran dokumen tersebut.

1.5 Manfaat Penelitian

Manfaat penelitian secara umum dapat berdampak kepada kepercayaan antara penerima dokumen terhadap pemilik yang mengeluarkan dokumen tersebut. Sehingga untuk setiap pihak yang berurusan dengan pemilik dokumen dapat meningkatkan kepercayaan terhadap dokumen yang dikeluarkan oleh pemilik dokumen.

1.6 Kerangka Pemikiran

Kerangka pemikiran pada Tabel 1.1 berisi gambaran kasar dari struktur tugas akhir yang berjudul Sistem Penjamin Integritas Dokumen Menggunakan Algoritma *Keccak* dan *Qrcode*. Berikut kerangka berpikir saya untuk penelitian ini.

Tabel 0.1 rangkaian kerangka pemikiran.

Problem
Penggunaan tanda tangan saja tidak cukup untuk menjamin sifat otentik dokumen, karena tanda tangan hanya bersifat otentik untuk pemilik tanda tangannya saja bukan dokumennya.

↓

Approach
Dibutuhkan sistem penanda baru yang bersifat autentik untuk dokumen, yaitu dengan menggunakan metode Hash Message Authentication Code.

↓

Software Development
Sistem akan dibangun dengan metode pengembangan *waterfall* menggunakan PHP.

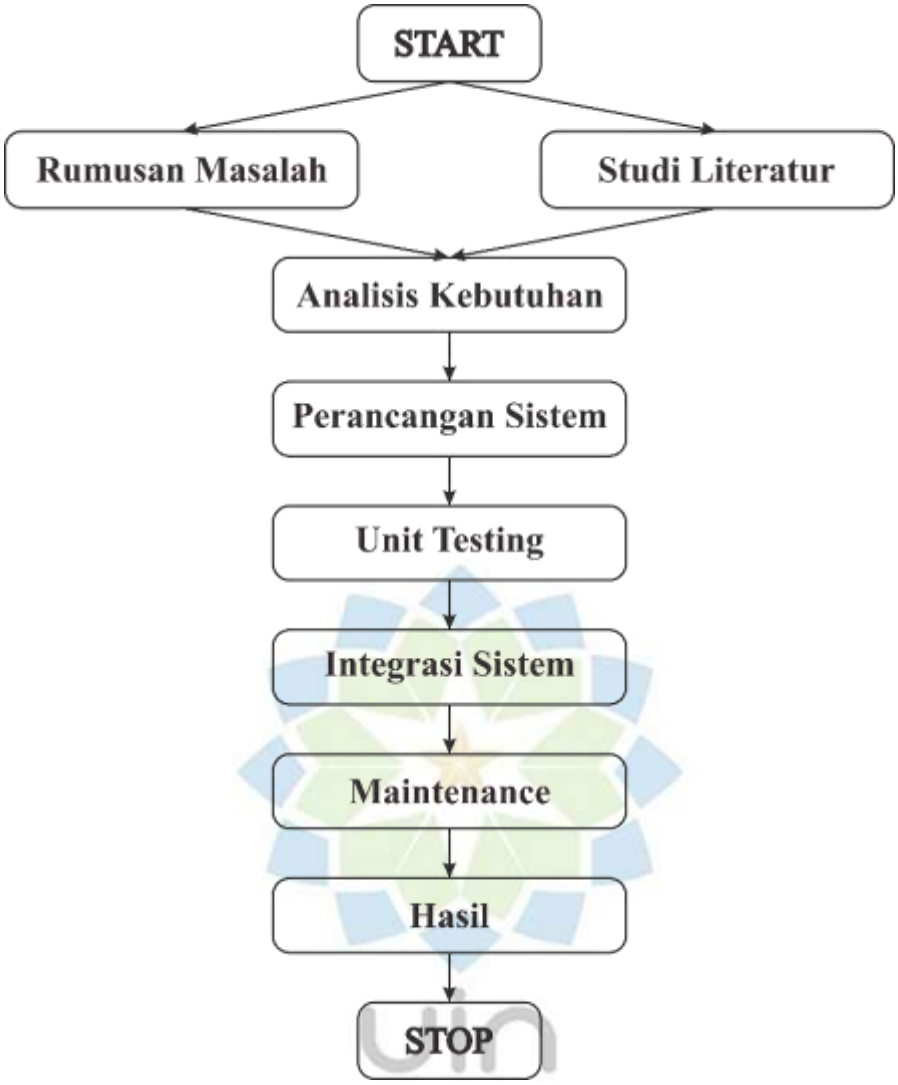
↓

Software Implementation
Keamanan dokumen dibantu dengan menambahkan *qrcode* pada dokumen dan mengacak dokumen tersebut dengan algoritma Keccak.

Result
Mengurangi risiko kejahatan dokumentasi dan kebenaran dokumen dapat di cek secara *online* pada aplikasi tersebut.

1.7 Metodologi

Metodologi penelitian berdasarkan kepada metode pengembangan perangkat lunak *waterfall*. Sesuai dengan artinya, metode ini bersifat berurutan (*sequential*) sehingga proses tidak akan bisa dimulai jika proses sebelumnya belum selesai [5]. Degan kata lain bahwa *output* dari proses sebelumnya akan menjadi *input* pada proses selanjutnya. Gambar 1.1 merupakan alur metodologi penelitian berdasarkan kepada metode pengembangan *waterfall*.



Gambar 0.1 alur metode penelitian.

1.7.1 Rumusan Masalah

Rumusan masalah mencakup rumusan masalah, tujuan dan Batasan dari penelitian dan metodologi yang akan digunakan pada penelitian ini. Perumusan masalah memberi petunjuk sebuah fenomena gap yaitu kesenjangan antara apa yang seharusnya terjadi dan apa yang benar-benar terjadi [6].

1.7.2 Studi Literatur

Sedangkan studi literatur adalah studi yang membahas teori-teori yang berhubungan tentang penelitian ini [6]. Hasil kajian dari rumusan masalah dan studi

literatur ini akan menghasilkan hipotesis. Hipotesis akan mengarahkan tujuan penelitian, menjelaskan fenomena dan mendorong munculnya teori. Hipotesis juga berpengaruh untuk menyempurnakan perumusan masalah, teori yang muncul dari hipotesis akan dibuktikan dengan data yang dikumpulkan pada penelitian.

Pengumpulan data dilakukan menggunakan metode studi dokumen. Studi dokumen adalah metode pengumpulan data dengan cara mempelajari data yang telah dibuat oleh subjek secara langsung atau pihak ketiga yang menjelaskan subjek tersebut, studi dokumen bersifat kualitatif.

1.7.3 Analisis Kebutuhan

Analisis Kebutuhan dan Definisi, layanan sistem, kendala, dan tujuan ditetapkan sesuai dengan hasil analisis data pada sistem yang ada. Mereka kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.

Hasil analisa informasi dari data yang didapatkan di atas, akan menjadi jawaban dari perumusan masalah dan mendukung tercapainya tujuan penelitian ini. *Output* dari solusi ini akan menjadi *input* untuk rancangan sistem sebagai fungsi yang harus dimiliki oleh sistem tersebut.

1.7.4 Rancangan Sistem

Rancangan Sistem dan Perangkat Lunak, proses desain sistem mengalokasikan kebutuhan baik untuk sistem perangkat keras atau perangkat lunak dengan membangun arsitektur sistem secara keseluruhan. Desain perangkat lunak melibatkan mengidentifikasi dan menjelaskan abstraksi sistem perangkat lunak dasar dan hubungannya.

1.7.5 Pengujian Unit

Implementasi dan Pengujian Unit, desain perangkat lunak diwujudkan sebagai sekumpulan program atau unit program. Pengujian unit melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya dan tujuannya.

1.7.6 Integrasi Sistem

Integrasi dan Pengujian Sistem, setiap unit program atau program individu terintegrasi dan diuji sebagai sistem yang lengkap untuk memastikan bahwa persyaratan perangkat lunak telah terpenuhi. Setelah pengujian, sistem perangkat lunak dikirimkan ke pelanggan.

1.7.7 Operasi dan Pemeliharaan

Operasi dan Pemeliharaan, sistem dipasang dan mulai digunakan secara praktis. Pemeliharaan melibatkan koreksi kesalahan yang tidak ditemukan pada tahap awal siklus hidup, meningkatkan implementasi unit sistem, dan meningkatkan layanan sistem saat persyaratan baru ditemukan. Namun fase ini tidak selalu dilakukan di beberapa kasus.

1.7.8 Hasil

Hasil mencakup kejadian pada saat penelitian dan penarikan kesimpulan. Melaporkan hambatan yang ditemui sehingga bisa menjadi *checkpoint* bagi penelitian dan pengembangan sistem ke depannya

1.8 Sistematika Penelitian

Penulisan laporan ini disusun dari lima BAB dengan susunan sebagai berikut:

1.8.1 Bab I Pendahuluan

Pendahuluan berisi tentang Latar Belakang, Perumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, Metodologi Tugas Akhir, Waktu dan Tempat Tugas Akhir, dan Sistematika Penulisan.

1.8.2 Bab II Landasan Teori

Teori, landasan, paradigma, cara pandang; Metode yang sudah ada dan atau akan digunakan; Konsep yang telah diuji kebenarannya.

1.8.3 Bab III Metodologi

Metode penelitian berdasarkan kepada siklus pengembangan sistem. Berdasar pada gambaran dari suatu permasalahan dan gambaran umum suatu obyek yang diteliti yaitu mengungkapkan permasalahan yang lebih khusus dari judul TA mencari alternatif pemecahan masalah, dirancang suatu pemecahannya yang mungkin (berupa pengembangan sistem yang sudah ada atau pembuatan sistem baru).

1.8.4 Bab IV Hasil dan Pembahasan

Bab ini memuat hasil dari implementasi dan pengujian perancangan yang telah dibuat.

1.8.5 Bab V Penutup

Berisi tentang kesimpulan dari keseluruhan hasil Tugas Akhir yang dilakukan penulis serta saran yang diajukan untuk *progress* dari jaringan komputer tersebut.