

**PENERAPAN *RIVEST SHAMIR ADLEMAN* UNTUK
VERIFIKASI TANDA TANGAN DIGITAL PADA LEMBAR
PENGESAHAN SKRIPSI**

PROPOSAL PENELITIAN



MUHAMMAD AKBAR

13020160073

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MUSLIM INDONESIA

MAKASSAR

APRIL 2021



**YAYASAN WAKAF UMI
UNIVERSITAS MUSLIM INDONESIA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA**

Kampus II UMI, Jl. Urip Sumoharjo KM. 05 Telp. (0411)447562, Makassar 90231

Bismillahirrohmanirrohiim

LEMBAR PENGESAHAN SEMINAR PROPOSAL

Nama : MUHAMMAD AKBAR
Stambuk : 13020160073
Program Studi : Teknik Informatika (S-1)
Judul Penelitian : PENERAPAN *RIVEST SHAMIR ADLEMAN*
UNTUK VERIFIKASI TANDA TANGAN
DIGITAL PADA LEMBAR PENGESAHAN
SKRIPSI

Berdasarkan Surat Penunjukan Dekan Fakultas Ilmu Komputer Universitas Muslim Indonesia Nomor : 0127/H.22/FIK-UMI/I/2020 tentang penetapan Dosen Pembimbing.

Makassar, 1 Juni 2021

Dosen Pembimbing

Pembimbing Utama

Pembimbing Pendamping

(Poetri Lestari L.B, S.Kom., M.T)

(Farniwati Fattah,S.T., M.T)

Mengetahui

Ketua Program Studi Teknik Informatika

(Tasrif Hasanuddin, S.T., M.Cs)



**YAYASAN WAKAF UMI
UNIVERSITAS MUSLIM INDONESIA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA**

Kampus II UMI, Jl. Urip Sumoharjo KM. 05 Telp. (0411)447562, Makassar 90231

KATA PENGANTAR

Bismillahir rohmani rohiim

Assalamu Alaikum Warahmatullahi Wabarakatuh.

Alhamdulillah Robbil 'alamin, segala puji bagi Allah Subhanallahu Wa Ta'ala, yang Maha Menciptakan, Menghidupkan dan Mematikan, yang Rahmat-Nya meliputi langit dan bumi, dunia dan akhirat dan kepada-Nyalah semua akan kembali. Shalawat serta salam semoga senantiasa terlimpahkan kepada Rasul yakni Nabi Muhammad Shallallahu 'Alaihi Wasallam, beserta seluruh keluarga dan para sahabat beliau yang telah mengorbankan harta, diri dan keluarga demi untuk perjuangan agama Islam.

Tak lupa penulis mensyukuri segala Rahmat dan Karunia yang telah dilimpahkan sehingga penulis dapat menyelesaikan proposal ini dengan judul “Penerapan Rivest Shamir Adleman Untuk Verifikasi Tanda Tangan Digital Pada Lembar Pengesahan Skripsi”. Proposal ini diajukan sebagai salah satu syarat dalam mencapai jenjang Sarjana Komputer (S1) yang nantinya dapat memberikan kontribusi kepada para pembacanya untuk dijadikan acuan dalam melakukan penelitian dibidang ilmu komputer kedepannya.

Berkat bimbingan dan bantuan dari berbagai pihak proposal ini dapat diselesaikan tepat pada waktunya. Oleh karena itu dengan hati yang tulus, penulis mengucapkan banyak terima kasih yang sebesar-besarnya. Terutama kepada orang tua penulis yaitu ayahanda H.Baharuddin dan ibunda HJ.Maslina yang selalu memberikan doa, kasih sayang dan dukungan baik moral maupun materil merupakan kekuatan besar bagi penulis untuk menyelesaikan proposal ini.

Proposal ini dapat penulis selesaikan dengan bantuan berbagai pihak, sehingga sudah sepantasnya penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. H. Basri Modding, SE., M.Si selaku Rektor Universitas Muslim Indonesia, beserta para Wakil Rektor.

2. Bapak Purnawansyah, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Muslim Indonesia, beserta para Wakil Dekan.
3. Bapak Tasrif Hasanuddin, S.T., M.Cs selaku Ketua Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Muslim Indonesia.
4. Ibu Poetri Lestari L.B, S.Kom., M.T selaku pembimbing utama yang telah banyak membantu dan membimbing dalam penyelesaian proposal ini.
5. Ibu Farniwati Fattah, S.T., M.T selaku pembimbing pendamping yang telah banyak membantu dan membimbing dalam penyelesaian proposal ini.
6. Seluruh dosen pengajar jurusan Teknik Informatika Universitas Muslim Indonesia Makassar, yang telah mendidik dan memberikan berbagai bekal pengetahuan yang tak ternilai harganya kepada penulis selama mengikuti perkuliahan.
7. Kepada seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah dengan tulus ikhlas memberikan doa dan motivasi kepada penulis sehingga dapat menyelesaikan tugas akhir.

Dengan begitu penulis menyadari bahwa dalam proposal ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan kritik dan saran yang mampu membangun penulis baik dari pembimbing, teman-teman dan pembaca untuk menyempurnakan proposal ini. Akhir kata semoga proposal ini dapat bermanfaat bagi masyarakat dan Mahasiswa Universitas Muslim Indonesia Makassar.

Wassalamu Alaikum Warahmatullahi Wabarakatuh.

Makassar, Mei 2021

Penulis

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN SEMINAR PROPOSAL	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL.....	vi
DAFTAR GAMBAR	vii
A. Latar Belakang.....	1
B. Rumusan Masalah	2
C. Batasan Masalah.....	2
D. Tujuan Penelitian.....	3
E. Manfaat Penelitian.....	3
F. Jadwal Penelitian	3
G. Tinjauan Pustaka	4
H. Landasan Teori	7
1. Tanda Tangan digital.....	7
2. Metode RSA.....	8
I. Metodologi Penelitian	9
1. Tahapan Penelitian	10
2. Instrumen Penelitian.....	22
J. Kerangka Pikir.....	23
DAFTAR PUSTAKA	25

DAFTAR TABEL

Tabel 1.	Jadwal Penelitian.....	3
Tabel 2.	Penelitian Terkait	4

DAFTAR GAMBAR

Gambar 1. <i>Use Case</i>	10
Gambar 2. <i>Activity diagram login</i>	11
Gambar 3. <i>Activity diagram mahasiswa</i>	12
Gambar 4. <i>Activity diagram dosen</i>	12
Gambar 5. <i>Activity diagram verifikasi</i>	14
Gambar 6. <i>Sequence diagram login</i>	14
Gambar 7. <i>Sequence diagram mahasiswa</i>	14
Gambar 8. <i>Sequence diagram dosen</i>	15
Gambar 9. <i>Sequence diagram verifikasi</i>	15
Gambar 1. <i>Class diagram</i>	16
Gambar 11. <i>ERD</i>	17
Gambar 12. <i>Desain database</i>	18
Gambar 13. <i>Interface form login</i>	19
Gambar 14. <i>Interface menu utama mahasiswa</i>	19
Gambar 15. <i>Interface menu utama dosen</i>	20
Gambar 16. <i>Interface verifikasi</i>	21

PENERAPAN *RIVEST SHAMIR ADLEMAN* UNTUK VERIFIKASI TANDA TANGAN DIGITAL PADA LEMBAR PENGESAHAN SKRIPSI

A. Latar Belakang

Pengesahan dokumen tugas akhir mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia telah dapat dilakukan secara digital, mahasiswa yang skripsinya telah disetujui oleh kedua pembimbingnya, cukup mengirimkan lembar pengesahan skripsi kepada dosen pembimbing dan ketua program studi melalui media *chat online* seperti Whatsapp maupun Telegram yang sudah familiar digunakan oleh masyarakat pada umumnya.

Adanya kemudahan menandatangani lembar pengesahan skripsi secara digital menimbulkan masalah yaitu tanda tangan digital dapat diduplikasi sehingga mudah sekali digunakan oleh pihak yang tidak bertanggung jawab. Oleh karenanya dibutuhkan sistem verifikasi untuk mengenali keabsahan lembar pengesahan skripsi. File yang digunakan dalam melengkapi tanda tangan digital lembar pengesahan skripsi berektensi pdf. Kecurangan selama ini terjadi adalah mahasiswa dapat mengajukan berkas pengurusan ijazah hanya dengan menambahkan tanda tangan dosen yang bersangkutan dari hasil menjiplak, meskipun revisi skripsi belum disetujui oleh dosen yang bersangkutan setelah mahasiswa melakukan ujian skripsi.

Sehingga dibutuhkan proses verifikasi terhadap lembar pengesahan skripsi mahasiswa, untuk pembuatan tanda tangan digital yaitu dengan membuat nilai *hash* yang mewakili keseluruhan dokumen lembar pengesahan skripsi, dimana nilai *hash* ini bersifat unik, kemudian nilai *hash* dienkripsi menggunakan kunci *private*, tanda tangan digital telah selesai dibuat. Proses verifikasi yaitu membandingkan tanda tangan digital yang telah didekripsi menggunakan kunci *public* dengan nilai *hash* lembar pengesahan skripsi. Jika tanda tangan digital sama dengan nilai *hash* lembar pengesahan skripsi, maka lembar pengesahan skripsi berhasil diverifikasi, jika nilainya tidak sama maka lembar pengesahan skripsi gagal dikonfirmasi sehingga skripsi tidak dapat diajukan sebagai salah satu berkas pengurusan ijazah.

Tanda tangan digital adalah sebuah kombinasi unik dari fungsi *hash* dan enkripsi dengan metode asimetris (Schneier, 1995), untuk enkripsi nilai *hash* penulis menggunakan metode *Rivest Shamir Adleman (RSA)* ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama *Rivest Shamir Adleman* sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, *RSA* mempunyai dua kunci, yaitu kunci *public* dan kunci *private*. *RSA* mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya (Ginting dkk, 2015).

Dengan menerapkan metode *RSA* untuk verifikasi tanda tangan digital pada lembar pengesahan skripsi, dapat menjadi salah satu solusi untuk mengecek keabsahan lembar pengesahan skripsi mahasiswa, sehingga dapat mencegah tindakan curang mengesahkan lembar pengesahan skripsi oleh pihak yang tidak bertanggung jawab tanpa sepengetahuan dosen yang bersangkutan.

B. Rumusan Masalah

Pada penelitian ini, rumusan masalah sebagai berikut:

1. Bagaimana merancang aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia menggunakan metode *RSA*?
2. Bagaimana menverifikasi keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia?

C. Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Menggunakan lembar pengesahan skripsi berekstensi pdf.

2. Perancangan aplikasi tanda tangan digital berbasis website.
3. Variabel verifikasi lembar pengesahan skripsi yaitu dengan membandingkan nilai tanda tangan digital dengan nilai hash lembar pengesahan skripsi

D. Tujuan Penelitian

Tujuan penelitian yang ingin dicapai adalah sebagai berikut:

1. Merancang aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa fakultas ilmu komputer menggunakan metode *RSA*
2. Verifikasi keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia

E. Manfaat penelitian

Manfaat dengan adanya aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa Ilmu Komputer Universitas Muslim Indonesia mampu menjadi salah satu solusi untuk menverifikasi keabsahan lembar pengesahan skripsi.

F. Jadwal Penelitian

Adapun jadwal penelitian yang dilakukan ditunjukkan pada Tabel 1.

Tabel 1. Jadwal Penelitian

No	Tahap Penelitian	Mei 2021				Juni 2021				Juli 2021				Agustus 2021				September 2021			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Identifikasi Masalah																				
2.	Analisis Kebutuhan Sistem																				
3.	Rancangan Sistem																				
4.	Implementasi Program																				

No	Tahap Penelitian	Mei 2021				Juni 2021				Juli 2021				Agustus 2021				September 2021			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
5.	Uji Coba Program (Testing)																				
6.	Penulisan laporan																				
7.	Pendadaran																				

G. Tinjauan Pustaka

Tinjauan pustaka ini terdiri dari beberapa jurnal sebagai referensi pelengkap guna terselesaikannya penelitian ini. Adapun beberapa penelitian yang terkait dengan penelitian ini ditunjukkan pada Tabel 2.

Tabel 2. Penelitian Terkait

No	Peneliti	Judul Penelitian	Hasil	Perbedaan
1	Azdy (2016)	Tanda tangan Digital Menggunakan Algoritma Keccak dan RSA	Pengujian penelitian ini memberikan hasil bahwa implementasi algoritme Keccak dan RSA pada tanda tangan digital dapat menjamin keaslian dokumen yang diterima, keabsahan pembuatan dokumen, dan anti penyangkalan oleh pembuat dokumen.	Pada penelitian sebelumnya menggunakan plain text untuk pembuatan tanda tangan digital, sedangkan penelitian penulis menggunakan dokumen pdf.
2	Isnaini (2017)	Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital	Tanda tangan digital yang dihasilkan berupa string ini dapat memastikan keaslian pesan yang dikirim jika memenuhi syarat, sehingga menjamin keamanan bertukar informasi dua pihak.	Pada penelitian sebelumnya menggunakan metode Schnorr untuk pembuatan tanda tangan digital, sedangkan penelitian penulis menggunakan metode <i>Rives Shamir Adelman</i>

No	Peneliti	Judul Penelitian	Hasil	Perbedaan
3	Abraham (2018)	Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur	Dari literatur yang sudah dikemukakan menunjukkan bahwa penggunaan TTD terbukti dapat mengurangi penggunaan kertas dimana dengan mengurangi kertas dan beralih ke dokumen elektronik sepenuhnya akan mewujudkan Green ICT, terutama di lingkungan pemerintah. Dengan Tanda Tangan Digital Akan mewujudkan kembali semangat awal pengembangan TIK, yaitu menjadikan teknologi yang ramah lingkungan. TTD di Indonesia juga sebaiknya memiliki peraturan sendiri dan memiliki peraturan yang mendukungnya yaitu Sistem Legal Digital dan Identitas Digital. Identitas Digital di Indonesia mungkin sudah diwakili oleh e-KTP, tetapi penggunaan e-KTP masih belum masif, dan harus dukung dengan kebijakan yang ada. Selain itu, dengan adanya peraturan yang kuat, akan sedikit memaksa para pengguna sistem elektronik untuk menggunakan TTD secara luas.	Pada penelitian sebelumnya berfokus pada teori tanda tangan digital sebagai solusi penggunaan kertas secara berlebihan. Pada penelitian penulis berfokus pada implementasi tanda tangan digital untuk verifikasi tanda tangan digital pada lembar pengesahan skripsi
4	Arifin dkk (2017)	Verifikasi Tanda Tangan Asli Atau Palsu Berdasarkan Sifat Keacakan (Entropi)	Sebaran nilai entropi tanda tangan asli menunjukkan bahwa 29 responden nilai entropinya mengumpul menjadi satu (dalam satu kelas) dan 1 responden nilai entropinya terpisah. Sebaran nilai entropi pada tanda tangan asli mempunyai error 3,31% dari total responden (30 responden). Nilai error 3,31% ini merupakan nilai entropi yang keluar kelompoknya atau kelasnya. Waktu perhitungan	Pada penelitian sebelumnya, proses verifikasi berdasarkan hasil <i>entropy</i> . Pada penelitian penulis untuk proses verifikasi berdasarkan hasil perbandingan nilai tanda tangan digital dengan nilai hash

No	Peneliti	Judul Penelitian	Hasil	Perbedaan
			nilai entropi pada tanda tangan palsu jika coretan atau piksel pada citra lebih besar dari citra tanda tangan asli maka waktu perhitungan nilai entropinya relatif lebih lama dibandingkan dengan citra tanda tangan asli	lembar pengesahan skripsi
5	Anshori dkk (2019)	Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital	<ol style="list-style-type: none"> 1. Aplikasi tanda tangan digital berhasil melakukan enkripsi pada dokumen sehingga menghasilkan tanda tangan digital 2. Pembangkitan kunci pada algoritma kriptografi RSA memastikan bahwa hanya pasangan kunci yang digunakan untuk proses enkripsi, yang dapat digunakan pada proses dekripsinya 3. Pengujian penelitian ini memberikan hasil bahwa aplikasi tanda tangan digital menggunakan algoritma kriptografi RSA dapat menjamin keamanan dokumen yang ditandatangani dalam aspek integrity, authentication, dan non-repudiation 	Pada penelitian sebelumnya, tidak menggunakan fungsi hash terhadap dokumen. Pada penelitian penulis, menambahkan fungsi hash
6	Ginting dkk (2015)	Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email	<ol style="list-style-type: none"> 1. Aplikasi yang menerapkan algoritma kriptografi RSA ini berjalan dengan baik mampu mengirim dan menerima email, dan dapat mengenkripsi dan dekripsi kotak masuk yang diterima 2. Dengan perangkat lunak ini, tujuan penelitian tercapai yaitu keamanan dalam menerima email terjamin. Ada pengamanan ganda untuk membuka pesan tersandi. Saat mendekripsi pesan yang telah dienkripsi harus memasukkan password terlebih dahulu, 	Pada penelitian sebelumnya menggunakan email sebagai objek penelitian, pada penelitian penulis objek penelitian pada lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia

No	Peneliti	Judul Penelitian	Hasil	Perbedaan
			<p>apabila masukan password salah pesan tidak akan didekripsi.</p> <p>3. Perangkat lunak ini hanya mengamankan isi pesan masuk email bukan mengamankan jalur transfer email</p> <p>4. Pada aplikasi yang dikembangkan ini, satu pesan asli dapat menghasilkan ciphertext yang berbeda-beda, karena proses pembangkitan kunci RSA didasarkan oleh nilai P dan Q yang acak</p> <p>5. Pesan kesalahan akan ditampilkan apabila terjadi kesalahan saat memasukkan suatu nilai yang salah saat enkripsi atau dekripsi pesan. Saat enkripsi masukan bit bernai kosong dan saat dekripsi masukan password salah</p>	

H. Landasan Teori

Dalam penelitian ini juga terdapat beberapa landasan teori yang digunakan serta dijadikan sebagai acuan dalam penelitian ini antara lain:

1. Tanda tangan digital

Tanda tangan digital merupakan mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan digital dapat digunakan untuk melakukan pembuktian secara matematis bahwa data tidak mengalami modifikasi secara illegal oleh pihak yang tidak bertanggung jawab, sehingga bisa digunakan sebagai salah satu solusi untuk melakukan verifikasi data

2. Metode RSA

Metode RSA di bidang kriptografi adalah sebuah algoritme pada enkripsi public key. RSA merupakan algoritma pertama yang cocok untuk *digital signature* seperti halnya enkripsi, dan salah satu yang paling maju dalam bidang kriptografi *public key* RSA masih digunakan secara luas dalam protokol *electronic commerce*, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

Proses pembentukan kunci *public* dan kunci *private* RSA adalah sebagai berikut (Agustina, 2015)

- a. Menentukan 2 bilangan prima, dengan nama p dan q. Misal nilai p = 51 dan q = 5.

- b. Menghitung nilai modulus (n) :

$$n = p \times q \quad (1)$$

$$n = 51 \times 5$$

$$n = 255$$

Keterangan:

n : Nilai modulus

- c. Menghitung nilai totient n :

$$(n) = (p - 1) \times (q - 1) \quad (2)$$

$$(n) = (51 - 1) \times (5 - 1)$$

$$(n) = (50 \times 4)$$

$$(n) = 200$$

- d. Menentukan nilai e dengan syarat $\gcd(e, (n)) = 1$ (3)

Keterangan:

e : bilangan prima, dan $1 < e < (n)$.

Pilih kunci publik e adalah 7 (relatif prima terhadap 200)

- e. Mencari nilai *deciphering exponent* (d), maka :

$$d = (1 + (k \times (n))) / e \quad (4)$$

$$d = (1 + (k \times 200)) / 7$$

Keterangan:

d : *deciphering exponent*

k : sembarang angka untuk pencarian hingga dihasilkan suatu nilai integer atau bulat

f. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai n, e, dan d telah didapatkan sehingga pasangan kunci telah terbentuk.

a) Pasangan kunci publik (n, e) = (255, 7)

b) Pasangan kunci rahasia (n, d) = (255, 343)

Proses Enkripsi metode *RSA* sebagai berikut (Agustina, 2015):

Plaintext : polsri

Nilai ASCII: p=112, o=111, l=108, s=115, r=114, i=105

Hasil enkripsi

Enkripsi *Rivest Shamir Adleman*

$112^7 \bmod 255 = 73$, pada tabel ascii adalah karakter I

$111^7 \bmod 255 = 36$, pada tabel ascii adalah karakter #

$108^7 \bmod 255 = 252$, pada tabel ascii adalah karakter w

$115^7 \bmod 255 = 55$, pada tabel ascii adalah karakter *n*

$114^7 \bmod 255 = 24$, pada tabel ascii adalah karakter (cancel)

$115^7 \bmod 255 = 45$, pada tabel ascii adalah karakter –

Proses dekripsinya adalah sebagai berikut (Agustina, 2015):

$75^{343} \bmod 255 = 112$, pada tabel ascii adalah karakter p

$36^{343} \bmod 255 = 36$, pada tabel ascii adalah karakter o

$252^{343} \bmod 255 = 252$, pada tabel ascii adalah karakter l

$55^{343} \bmod 255 = 55$, pada tabel ascii adalah karakter s

$24^{343} \bmod 255 = 24$, pada tabel ascii adalah karakter r

$45^{343} \bmod 255 = 45$, pada tabel ascii adalah karakter i

I. Metodologi Penelitian

Metodologi penelitian penulis terdiri atas tahap penelitian, dan instrumen penelitian sebagai berikut:

1. Tahap Penelitian

Dalam penelitian yang penulis lakukan terbagi menjadi beberapa tahap penelitian yaitu :

a. Identifikasi masalah

Pada tahap ini penulis melakukan wawancara kepada beberapa alumni mengenai permasalahan yang ditemui selama meminta tanda tangan persetujuan lembar pengesahan skripsi kepada dosen bersangkutan di Fakultas Ilmu Komputer Universitas Muslim Indonesia

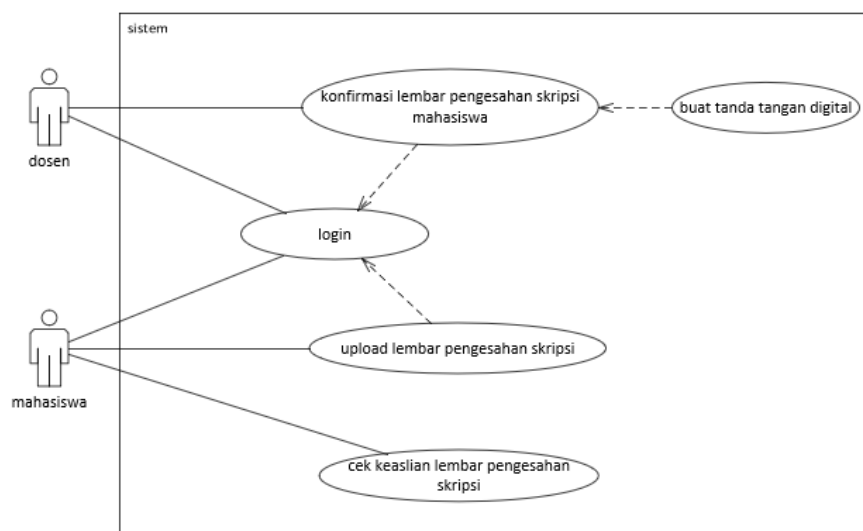
b. Analisis kebutuhan sistem

Pada analisis kebutuhan sistem peneliti melakukannya pada peneliti akan menganalisis apa saja yang dibutuhkan sistem dalam proses pengembangannya menjadi sebuah aplikasi tanda tangan digital lembar pengesahan skripsi seperti spesifikasi perangkat keras dan perangkat lunak seperti yang terlihat pada instrument penelitian.

c. Rancangan sistem

Pada tahapan rancangan sistem penulis akan menganalisis dan merancang interface, desain database, dan pemodelan sistem menggunakan *Unified Modeling Language*.

1) Use Case Diagram



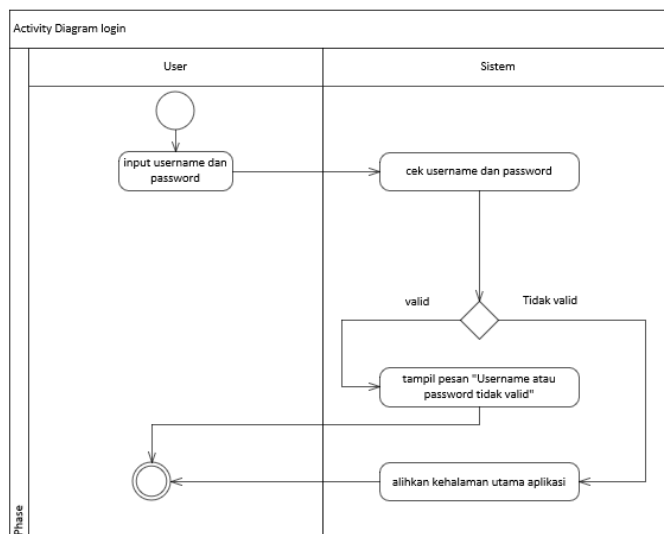
Gambar 1 Use case diagram

Pada Gambar 1 *use case diagram*, berikut ini adalah penjelasnya:

- a) Agar dosen dan mahasiswa dapat masuk ke fitur utama aplikasi, terlebih dahulu harus login
- b) Dosen mengkonfirmasi lembar pengesahan skripsi mahasiswa, agar sistem dapat membuat tanda tangan digital
- c) Mahasiswa dapat meng-*upload* lembar pengesahan skripsi
- d) Mahasiswa dapat verifikasi lembar pengesahan skripsi tanpa harus login

2) Activity Diagram

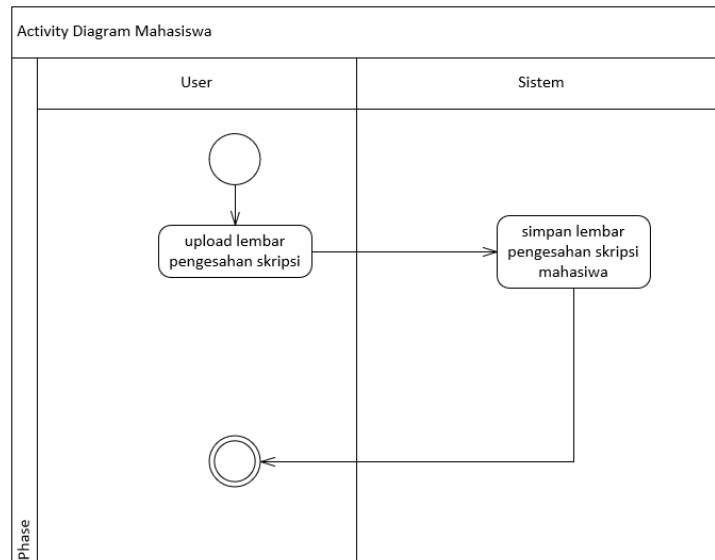
– Login



Gambar 2 Activity diagram login

Pada Gambar 2, *user* memasukkan *username* dan *password*, kemudian sistem cek *username* dan *password*, jika valid arahkan ke halaman utama aplikasi, jika tidak valid tampilkan pesan “*Username dan password tidak valid*”

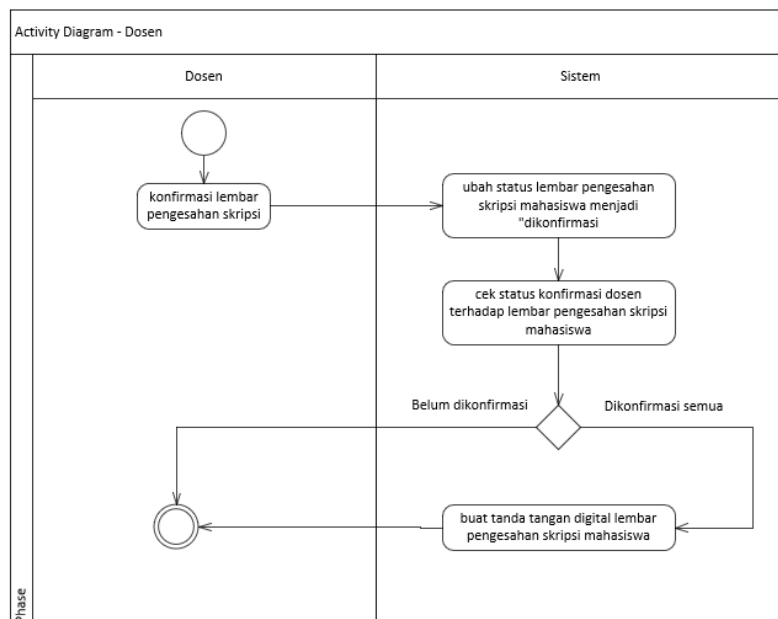
– Mahasiswa



Gambar 3 Activity diagram mahasiswa

Pada gambar 3, Mahasiswa *upload* lembar pengesahan skripsi, kemudian sistem akan menyimpan dokumen tersebut kedalam sistem

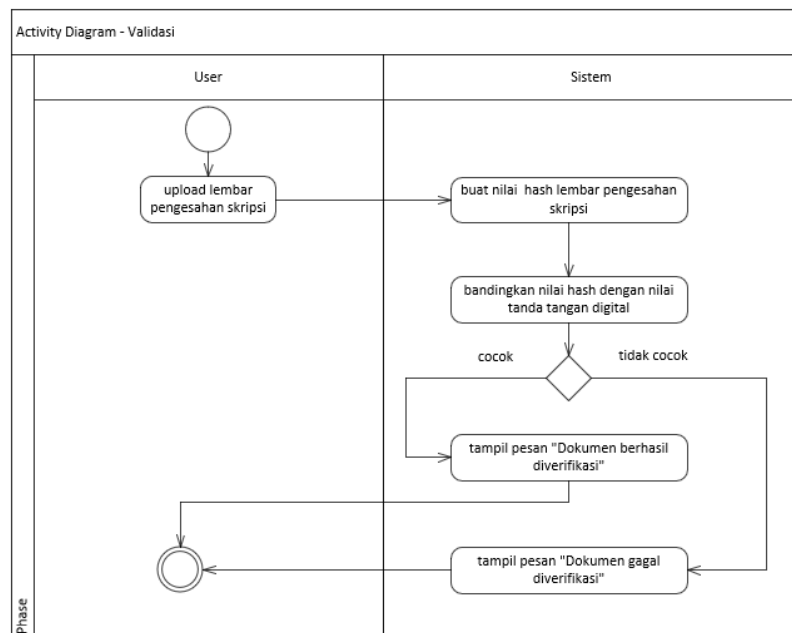
– Dosen



Gambar 4 Activity diagram dosen

Pada gambar 4, dosen konfirmasi lembar pengesahan skripsi mahasiswa, kemudian sistem mengubah status konfirmasi lembar pengesahan skripsi mahasiswa menjadi “dikonfirmasi”, jika semua dosen telah melakukan konfirmasi, maka sistem membuat tanda tangan digital, jika belum terkonfirmasi semua maka proses selesai

– Verifikasi

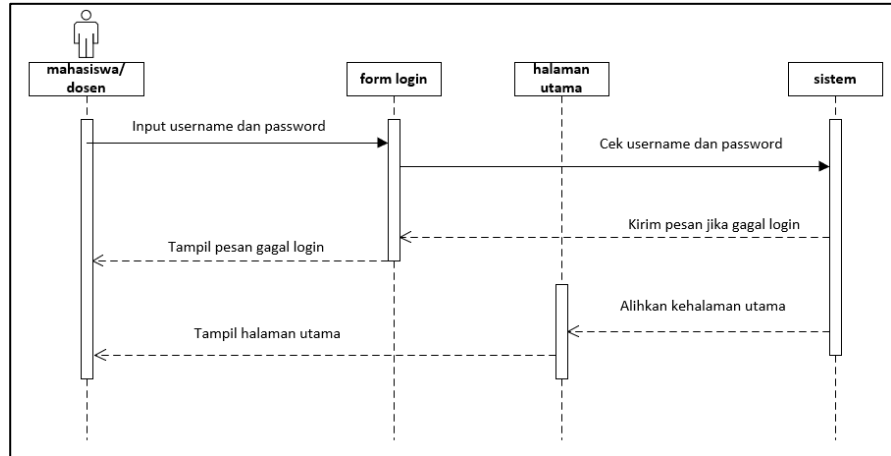


Gambar 5 Activity diagram verifikasi

Pada gambar 5, mahasiswa *upload* lembar pengesahan skripsi, selanjutnya sistem membuat nilai hash, kemudian sistem membandingkan nilai *hash* lembar pengesahan skripsi dengan nilai tanda tangan digital lembar pengesahan skripsi

3) Sequence Diagram

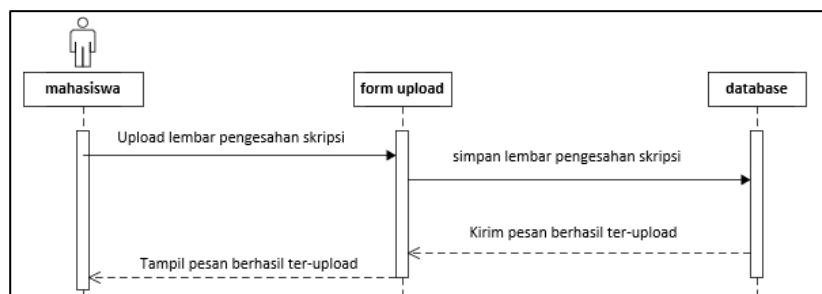
– Login



Gambar 6 Sequence diagram login

Pada gambar 6, user memasukkan *username* dan *password* pada form login, kemudian sistem mengecek *username* dan *password*, jika gagal tampilkan pesan gagal login, jika berhasil, sistem mengalihkan kehalaman utama aplikasi dan menampilkan halaman utama aplikasi

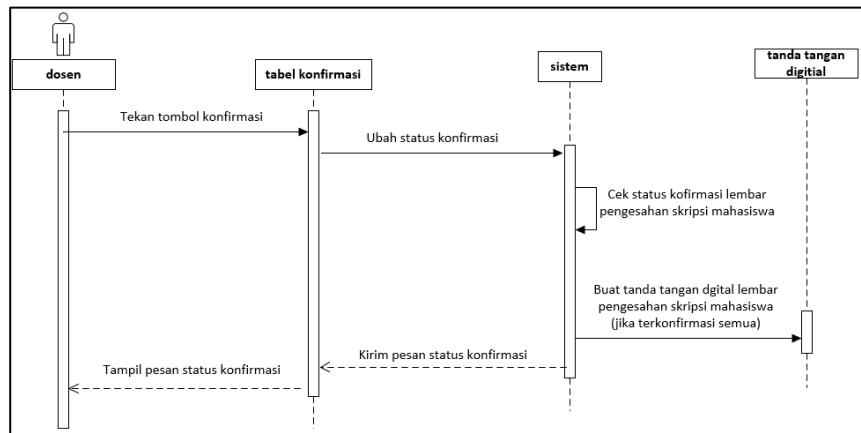
– Mahasiswa



Gambar 7 Sequence diagram mahasiswa

Pada gambar 7, Mahasiswa *upload* lembar pengesahan skripsi, kemudian sistem menyimpan lembar pengesahan skripsi kedalam database, selanjutnya mengirim pesan berhasil ter-*upload*, kemudian akan tampil pesan pada form upload yang dilihat oleh mahasiswa.

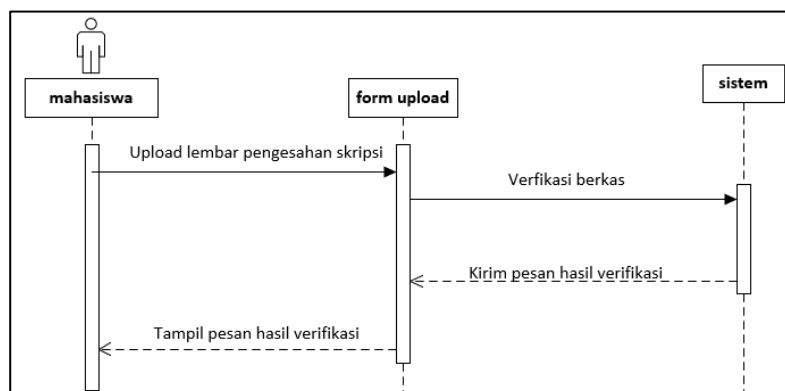
– Dosen



Gambar 8 *Sequence diagram* dosen

Pada gambar 4, dosen tekan tombol konfirmasi pada tabel konfirmasi, kemudian sistem mengubah status konfirmasi lembar pengesahan skripsi mahasiswa menjadi “dikonfirmasi”. Sistem cek status konfirmasi lembar pengesahan skripsi mahasiswa, sistem membuat tanda tangan digital jika lembar pengesahan skripsi mahasiswa telah dikonfirmasi oleh semua dosen. Sistem mengirim status konfirmasi dan menampilkannya kepada mahasiswa

– Verifikasi

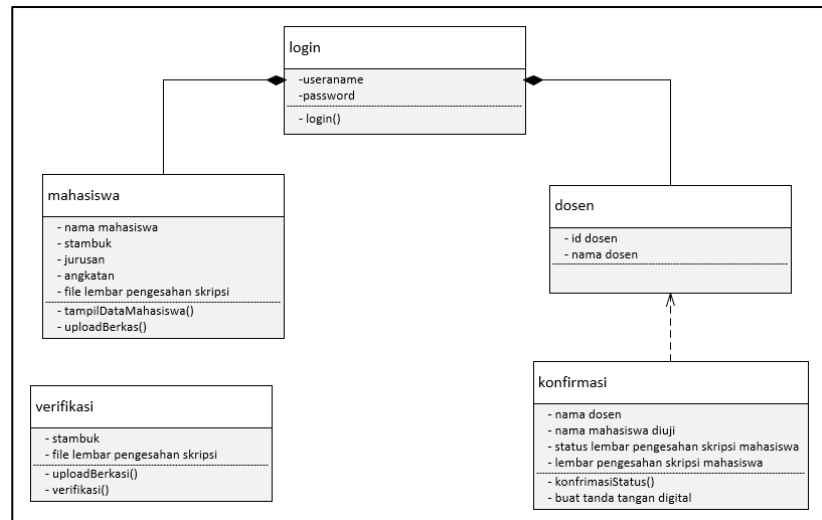


Gambar 9 *Sequence diagram* verifikasi

Pada gambar 9, mahasiswa *upload* lembar pengesahan skripsi, selanjutnya sistem melakukan verifikasi berkas, kemudian

sistem mengirimkan hasil verifikasi dan menampilkan hasil verifikasinya kepada mahasiswa.

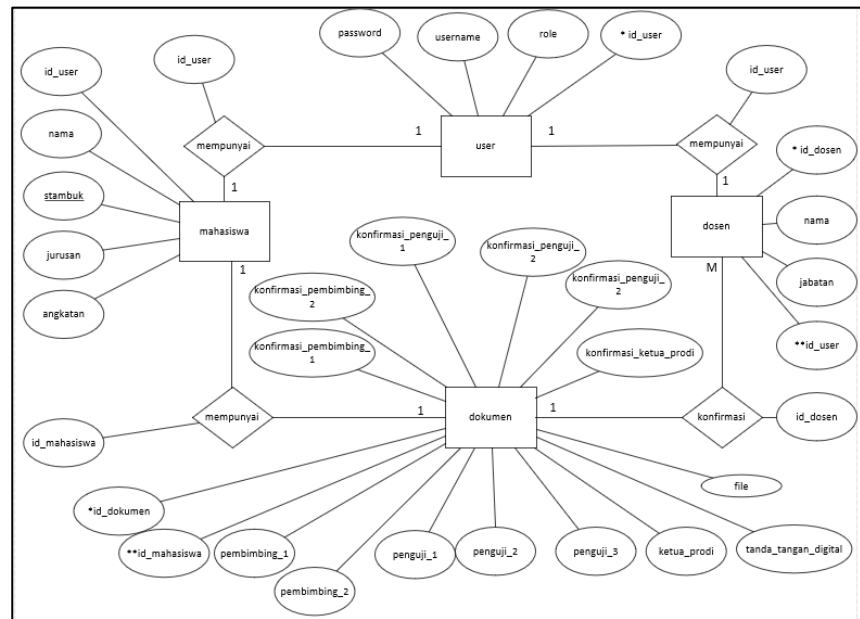
4) Class Diagram



Gambar 10 *Class diagram*

Pada gambar 10 agar dapat mengakses mahasiswa, dosen, dan konfirmasi terlebih dahulu harus login, selanjutnya pada kelas konfirmasi dependensi terhadap kelas dosen karena untuk menjalankan fungsi `konfirmasiStatus()` bergantung pada kelas dosen. Kelas mahasiswa terdapat dua fungsi dimana dapat melihat data mahasiswa yang telah login, dan fungsi untuk meng-*upload* berkas. Kelas verifikasi merupakan kelas yang berdiri sendiri dan tidak bergantung pada kelas manapun, pada kelas verifikasi terdapat dua fungsi yaitu *upload* berkas dan fungsi untuk verifikasi untuk mengecek keabsahan lembar pengesahan skripsi.

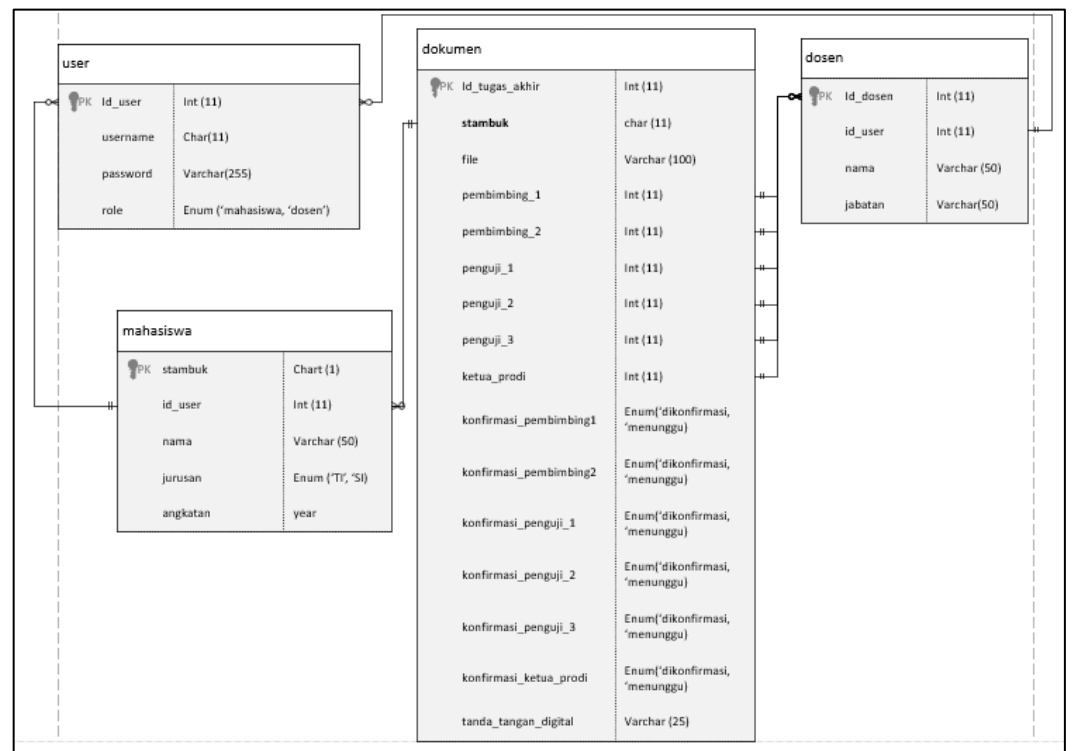
5) ERD (Entity Relational Diagram)



Gambar 11 ERD

Pada gambar 11 terdapat beberapa *entity* yaitu user, mahasiswa, dosen, dan dokumen. Entitas mahasiswa mempunyai akun pada entitas user yang dihubungkan oleh atribut id_user, dimana satu mahasiswa hanya boleh memiliki satu akun user pada entitas user. Entitas mahasiswa mempunyai dokumen lembar pengesahan skripsi pada entitas dokumen yang dihubungkan oleh atribut stambuk, dimana setiap mahasiswa hanya boleh memiliki satu dokumen lembar pengesahan skripsi pada entitas dokumen. Entitas dosen mempunyai akun pada entitas user yang dihubungkan oleh atribut id_user, dimana satu dosen hanya boleh memiliki satu akun user pada entitas user, selanjutnya entitas dosen konfirmasi dokumen lembar pengesahan skripsi pada entitas dokumen yang dihubungkan oleh atribut id_dosen, dimana banyak dosen konfirmasi satu dokumen lembar pengesahan skripsi pada entitas dokumen.

6) Desain Database

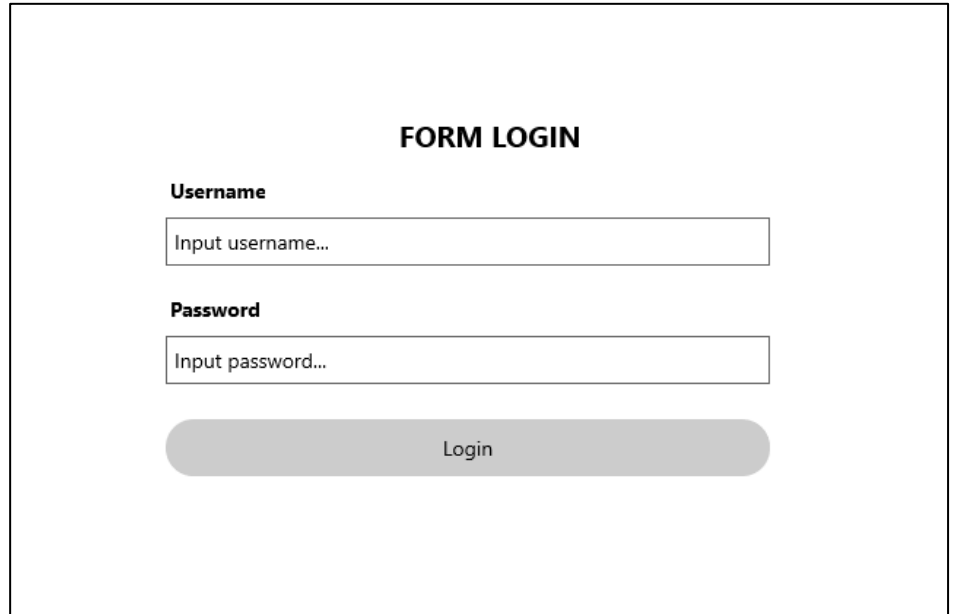


Gambar 12 Desain database

Pada gambar 11 terdapat beberapa tabel yaitu user, mahasiswa, dosen, dan dokumen. Tabel user berelasi dengan tabel mahasiswa, dan tabel dosen yang dihubungkan oleh id_user dengan tipe int yang panjang valuenya yaitu sebelas. Tabel mahasiswa berelasi dengan tabel dokumen yang dihubungkan oleh stambuk. Tabel dosen berelasi dengan tabel dokumen yang dihubungkan oleh id_dosen.

1) Perancangan *Interface*

– Login

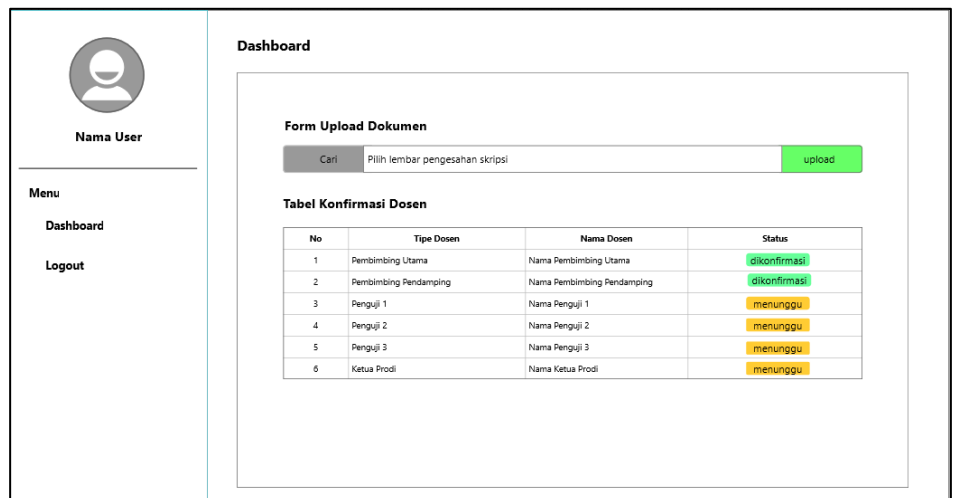


The screenshot shows a login form titled "FORM LOGIN". It contains two input fields: "Username" with the placeholder text "Input username..." and "Password" with the placeholder text "Input password...". Below these fields is a rounded rectangular button labeled "Login".

Gambar 13 *Interface* form login

Pada gambar 13 mahasiswa atau dosen yang akan login harus memasukkan username dan password, kemudian tombol login berfungsi untuk melakukan login.

– Mahasiswa



The screenshot shows a student dashboard. On the left is a sidebar with a user profile icon and the text "Nama User". Below this is a "Menu" section with links for "Dashboard" and "Logout". The main content area is titled "Dashboard" and contains a "Form Upload Dokumen" section with a search bar (placeholder: "Cari"), a text input (placeholder: "Pilih lembar pengesahan skripsi"), and an "upload" button. Below this is a "Tabel Konfirmasi Dosen" section with a table showing the status of document uploads for various roles.

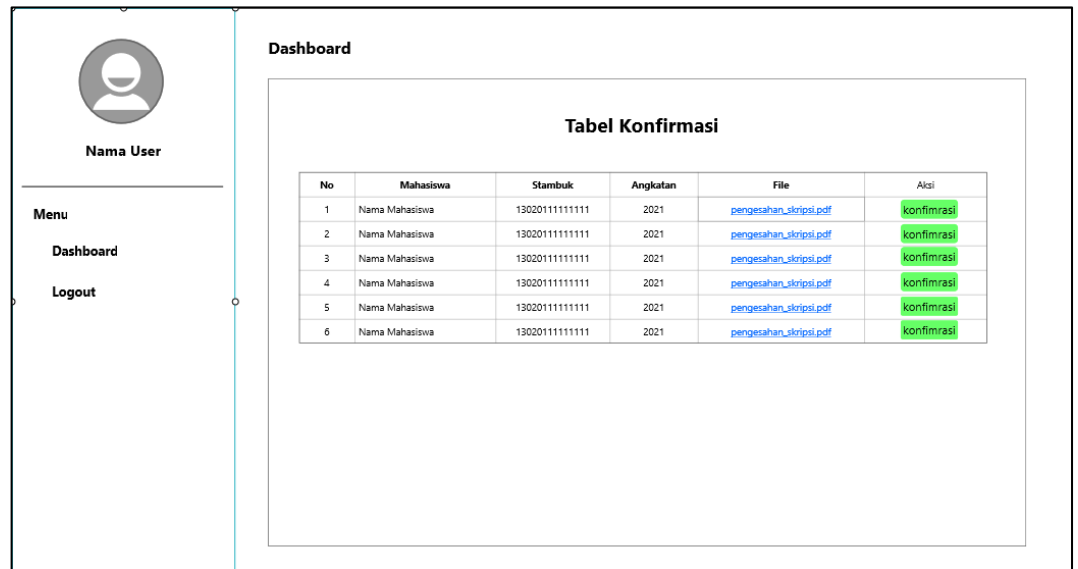
No	Tipe Dosen	Nama Dosen	Status
1	Pembimbing Utama	Nama Pembimbing Utama	dikonfirmasi
2	Pembimbing Pendamping	Nama Pembimbing Pendamping	dikonfirmasi
3	Penguji 1	Nama Penguji 1	menunggu
4	Penguji 2	Nama Penguji 2	menunggu
5	Penguji 3	Nama Penguji 3	menunggu
6	Ketua Prodi	Nama Ketua Prodi	menunggu

Gambar 14 *Interface* menu utama mahasiswa

Pada gambar 14 terdapat dua menu yaitu *dashboard*, dan *logout*. Menu *dashboard* terdapat form untuk meng-upload

lembar pengesahan skripsi mahasiswa, dan tabel konfirmasi dosen untuk mengecek status konfirmasi lembar pengesahan skripsi yang telah diupload. Menu *logout* untuk keluar dari menu utama aplikasi

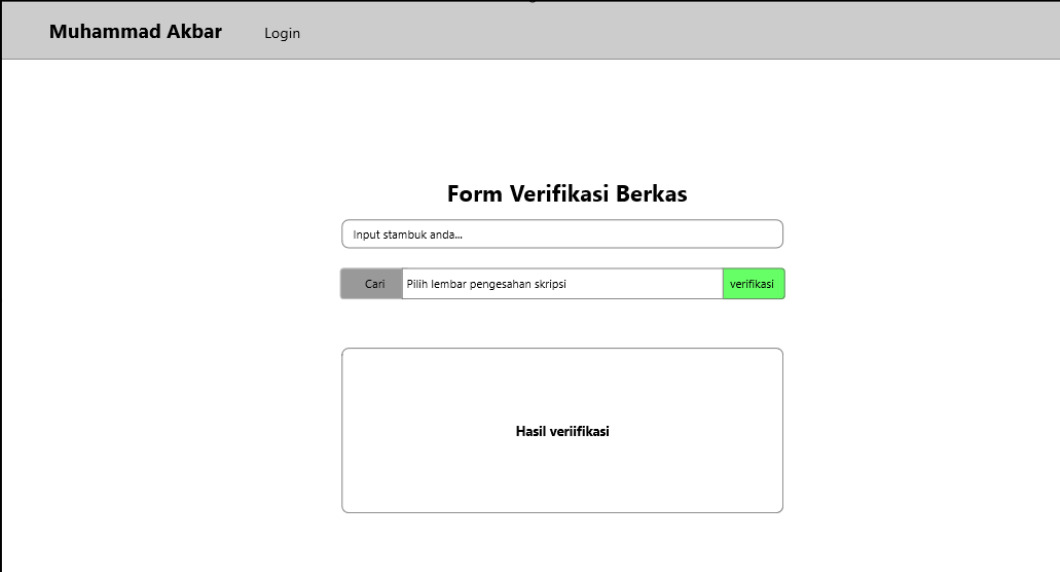
– Dosen



Gambar 15 Interface menu utama dosen

Pada gambar 15 terdapat dua menu yaitu *dashboard*, dan *logout*. Menu *dashboard* terdapat tabel konfirmasi untuk mengkonfirmasi lembar pengesahan skripsi mahasiswa, dan pada kolom file terdapat link untuk melihat lembar pengesahan skripsi mahasiswa. Menu *logout* untuk keluar dari menu utama aplikasi

– Verifikasi



The screenshot displays a web interface for document verification. At the top, a header bar contains the name 'Muhammad Akbar' and a 'Login' link. The main content area is titled 'Form Verifikasi Berkas'. It includes an input field for 'Input stambuk anda...', a 'Cari' button, a text field for 'Pilih lembar pengesahan skripsi', and a green 'verifikasi' button. Below these elements is a large rectangular box labeled 'Hasil verifikasi'.

Gambar 16 *Interface verifikasi*

Pada gambar 16 terdapat form verifikasi untuk melakukan verifikasi dimana mahasiswa memasukkan stambuk, *upload* lembar pengesahan skripsi, saat menekan tombol verifikasi sistem akan melakukan verifikasi dokumen dan menampilkan hasilnya pada kotak hasil verifikasi.

d. Implementasi program

Pada tahap ini peneliti telah masuk ketahap pembuatan aplikasi tanda tangan digital lembar pengesahan skripsi menggunakan bahasa pemrograman PHP.

e. Uji Coba Program (*Testing*)

Pada tahap ini peneliti akan melakukan pengujian fitur-fitur aplikasi agar aplikasi sesuai dengan rancangan bangun program

f. Penulisan Laporan

Pada tahap ini peneliti menulis laporan berdasarkan penelitian yang telah dilakukan

g. Pendadaran

Setelah menulis laporan penelitian, maka peneliti akan memasuki tahap akhir yaitu mempresentasikan hasil penelitian yang telah dilakukan.

2. Instrumen Penelitian

Instrumen penelitian adalah alat bantu yang dipilih dalam kegiatannya agar sistematis dan mempermudah peneliti selama melakukan penelitian. Instrumen ini terbagi menjadi dua yaitu:

a. Perangkat Keras (*Hardware*)

Perangkat keras atau *Hardware* yang digunakan dalam pengembangan aplikasi adalah:

1. *Processor* minimal *core i3*.
2. Memory (RAM) minimal 4,00 GB.

b. Perangkat Lunak (*Software*)

Perangkat lunak atau *software* yang digunakan adalah:

1. Sistem operasi Microsoft Windows 10 Professional 64-bit,
2. Code editor Visual Studio Code versi 1.39.1 64-bit
3. Database Mysql, menggunakan Xampp versi 7.1.9.0.,
4. Browser versi 72.0.3626.119,
5. Environment bahasa pemrograman yaitu PHP

J. Kerangka Pikir

Judul Penelitian

Penerapan Tanda Tangan Digital Untuk Verifikasi Lembar Pengesahan Skripsi Menggunakan Metode *Rivest Shamir Adleman*



Latar Belakang

Dengan adanya kemudahan menandatangani lembar pengesahan skripsi secara elektronik juga memiliki kekurangan yaitu tanda tangan dapat diduplikasi sehingga dapat digunakan oleh pihak yang tidak bertanggung jawab untuk menandatangani lembar pengesahan skripsi tanpa sepengetahuan pemilik tanda tangan, sehingga lembar pengesahan skripsi yang telah ditanda tangani tidak dapat diverifikasi untuk menjamin keabsahannya. Dengan menerapkan metode *rivest shamir adleman* untuk verifikasi tanda tangan digital pada lembar pengesahan skripsi, dapat menjadi salah satu solusi untuk mengecek keabsahan lembar pengesahan skripsi mahasiswa, sehingga dapat mencegah tindakan curang mengesahkan lembar pengesahan skripsi oleh pihak yang tidak bertanggung jawab tanpa sepengetahuan dosen yang bersangkutan.



Metode Penelitian

Dalam penelitian ini, metode penelitian yang digunakan adalah penelitian tindakan (*action research*), menurut Hasibuan (2007) penelitian tindakan merupakan “penelitian yang berfokus langsung pada tindakan sosial. Penelitian tindakan ini merupakan metode yang didasarkan pada tindakan masyarakat yang seringkali diselenggarakan pada suatu latar yang luas, seperti di rumah sakit, pabrik, sekolah, dan lain sebagainya”. Metode penelitian tindakan diduga kuat sesuai dengan permasalahan yang diteliti penulis karena didasarkan pada permasalahan penggunaan tanda tangan elektronik yang tidak dapat menjamin keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia, dan untuk pembuatan tanda tangan digital menggunakan metode *RSA*



Tujuan Penelitian

- a. Merancang aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia menggunakan metode *RSA*.
- b. Verifikasi keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia.



Hasil Penelitian

1. Telah mampu merancang aplikasi tanda tangan digital menggunakan metode *RSA*.
2. Aplikasi tanda tangan digital yang dapat memverifikasi keabsahan dokumen lembar pengesahan skripsi mahasiswa menggunakan metode *RSA*.

DAFTAR PUSTAKA

- Schneier, B. 1995. *Applied Cryptography (2Nd Ed.): Protocols, Algorithms, and Source Code in C*. New York, NY, USA: John Wiley & Sons, Inc.
- Romine, C, H. 2015. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*
- Ginting, Albert., Isnanto R. Rizal., Windasari, Ike Pertiwi. 2015. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, Vol 3, No.2.
- Abraham, F. Z., Santosa, P. I. and Winarno, W. W. 2018. Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (Tik) Hijau : Sebuah Kajian Literatur, pp. 111–124.
- Agustina, A. N. 2015. Pengamanan Dokumen Menggunakan Metode Rsa (Rivest Shamir Adleman) Berbasis Web, pp. 14–19.
- Anshori, Y., Erwin Dodu, A. Y. and Wedananta, D. M. P. 2019. Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital, *Techno.Com*, pp. 110–121.
- Arifin, J. and Zidny, M. 2017. Verifikasi Tanda Tangan Asli Atau Palsu Berdasarkan Sifat Keacakan (Entropi).
- Azdy, R. A. 2016. ‘Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA. pp. 184–191.
- Isnaini, H. F., Karyati, K. and Matematika, J. P. 2017. Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital Implementation of Schnorr Signature Scheme in The Form of Digital Signature, pp. 57–64.
- Nazal, M. A., Pulungan, R. and Riasetiawan, M. 2019. Data Integrity and Security using Keccak and Digital Signature Algorithm (DSA)’, *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, 13(3), pp. 273.
- Hasibuan, Zainal A. 2007. *Metodologi Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi*. Fakultas Ilmu Komputer Universitas Indonesia.