JURNAL PENDIDIKAN DAN APLIKASI INDUSTRI
Vol. 10 No. 2 2023 : 84 - 93
p-ISSN : 0126 – 4036 e-ISSN : 2716 – 0416

Sistem Tanda Tangan Digital Menggunakan SHA-3 dan ECDSA

Ade Ismail[1], Vipkas Al Hadid F[2], Anissa Taufika F[3]

[1,2,3] *Jurusan Teknologi Informasi, Politeknik Negeri Malang, Jawa Timur, Indonesia*

[1] aismail@polinema.ac.id, [2] vipkas@polinema.ac.id, [3]annisa.taufika@polinema.ac.id

Article History:
Received 17 Jun 2023
Revised 26 Juli 2023
Accepted 26 Juli 2023
Available online 04 Oktober 2023

Abstrak
Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan dokumen digital menggunakan digital signature berbasis ECDSA (Elliptic Curve Digital Signature Algorithm) dan SHA-3 (Secure Hash Algorithm 3). Metode penelitian yang digunakan adalah eksperimen kontrol acak dalam lingkungan simulasi. Data yang diperoleh dari eksperimen ini dianalisis secara statistik untuk mengukur efektivitas sistem keamanan.Hasil penelitian menunjukkan bahwa implementasi digital signature ECDSA dan SHA-3 secara signifikan meningkatkan keamanan dan integritas dokumen digital. Ditemukan bahwa tingkat keberhasilan verifikasi dan otentikasi dokumen mencapai 100%, mengkonfirmasi keefektifan digital signature ECDSA dalam memastikan keutuhan dan keabsahan tanda tangan digital. Algoritma hash SHA-3 yang kuat juga memberikan tingkat integritas yang tinggi dengan menghasilkan *hash* (kata sandi) yang unik dan sulit diretas. Selain itu, implementasi ini juga mempercepat proses tanda tangan digital dengan rata-rata waktu tanda tangan sebesar 0,00286 detik. Efisiensi dalam penggunaan sistem keamanan ECDSA dan SHA-3 terlihat dari penghematan waktu yang signifikan pada proses tanda tangan.

Kata Kunci : digital *signature*, dokumen digital, ECDSA, keamanan informasi, SHA-3.

Abstract
The purpose of this study is to develop a system for digital document security using a digital signature based on the Secure Hash Algorithm-3 (SHA-3) and the Elliptic Curve Digital Signature Algorithm (ECDSA). The method of data collection used is experiment control of an acak in a simulated environment. To assess the effectiveness of the keamanan system, statistics are used to the data from this experiment.The study's findings indicate that using digital signatures like ECDSA and SHA-3 significantly improves the security and reliability of electronic documents. It is understood that the percentage of successful document verification and authentication exceeds 100%, confirming the effectiveness of the ECDSA digital signature in assuring the integrity and authenticity of digital signatures. The strong SHA-3 hash algorithm also provides a high level of integrity by producing a unique and weakly direct hash. In addition to that, this implementation also speeds up the digital time stamping process by around 0,00286 seconds. Efficiency in the use of the ECDSA and SHA-3 key management systems may be seen in the reduction of significant processing time during the signatures process.
Keywords : *digital documents, digital signatures, ECDSA, information security, SHA-3.*

1. Pendahuluan

Dalam era digital saat ini, penggunaan dokumen digital telah menjadi hal yang umum dalam berbagai bidang, seperti bisnis, pemerintahan, dan akademik. Dokumen digital memberikan kemudahan akses, pertukaran informasi yang cepat, dan efisiensi dalam penyimpanan data(Nuraeni et al., 2020). Beberapa manfaat seperti efisiensi waktu, pengurangan biaya, dan peningkatan keamanan dan integritas dokumen menjadi hal yang bisa diambil(Yuniati & Sidiq, 2020).

Namun, seiring dengan peningkatan penggunaan dokumen digital, tantangan keamanan yang serius juga muncul. Keamanan informasi dalam dokumen digital menjadi hal yang sangat penting untuk melindungi integritas, kerahasiaan, dan keaslian data yang disimpan(Pittalia, 2019). Salah satu mekanisme keamanan yang penting dalam konteks ini adalah digital *signature* atau tanda tangan

digital. Digital *signature* memungkinkan verifikasi keaslian dan integritas dokumen digital, serta memastikan bahwa dokumen tersebut tidak mengalami perubahan yang tidak sah(Sarasvananda & Iswara, 2022)(Triand et al., 2019). Tanda tangan digital juga menghilangkan resiko dokumen rusak, hilang, atau dibuat tanpa izin oleh pihak ketiga yang kerap terjadi pada dokumen kertas(Cahyadi, 2020).

Beberapa penelitian sebelumnya telah mengkaji penggunaan digital *signature* dalam sistem keamanan dokumen digital. Anshori dkk, mengimplementasikan algoritma kriptografi RSA pada tanda tangan digital (Anshori et al., 2019), sedangkan Arwa dkk, menggunakan algoritma ECDSA pada dokumen tipe PDF (Arwa et al., 2021). Penelitian lainnya mengusulkan penggunaan algoritma keccak dan RSA dalam tanda tangan digital(Seta et al., 2020). Penelitian ini menunjukkan bahwa digital *signature* dapat digunakan sebagai mekanisme keamanan yang efektif dalam melindungi dokumen digital dari perubahan yang tidak sah. Penelitian lainnya mengimplementasikan algoritma hash SHA memiliki hasil *chippertext* yang sulit ditebak oleh *hacker* karena data yang dihasilkan tidak mungkin sama(Sinduningrum, 2019). Perbandingan metode antara Enkripsi RC4, SHA, dan MD5 bahwa algoritma SHA memiliki tingkat kekuatan yang lebih baik daripada metode RCA dan MD5, sehingga algoritma SHA direkomendasikan untuk digunakan dalam sistem keamanan data.

Terdapat varian Algoritma SHA yaitu SHA-0, SHA-1, SHA-2 dan SHA-3. Berdasarkan penelitian sebelumnya yang berjudul Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 dijelaskan bahwa penggunaan algoritma SHA-1 ditemukan kelemahan dalam mengamankan password pengguna yang tersimpan di database, sehingga penulis menggantikan algoritma SHA-1 tersebut dengan algoritma SHA-3. Algoritma SHA-3 dapat digunakan untuk menjamin kerahasiaan dan keutuhan data(Sari, 2021). Serta dari pengujian *brute-force, avalanche effect*, dan pengujian waktu pemrosesan menunjukkan bahwa algoritma SHA-3 memiliki kinerja dan ketahanan yang lebih baik daripada algoritma SHA-1(Fitriani et al., 2021).

Dalam artikel ini, kami mengusulkan implementasi sistem keamanan informasi dokumen digital menggunakan digital *signature* berbasis algoritma ECDSA (*Elliptic Curve Digital Signature Algorithm*) dan SHA-3 (Secure Hash Algorithm 3). Pendekatan dual *signature* ECDSA memberikan lapisan perlindungan tambahan dengan membagi proses penandatanganan menjadi dua tahap, sehingga tidak ada entitas tunggal yang memiliki tanda tangan lengkap (genc & Cañavate-Sanchez, 2020). Kebaruan ilmiah artikel ini terletak pada penggabungan kedua algoritma ini dalam konteks keamanan dokumen digital. Melalui penggunaan ECDSA, tanda tangan digital dapat dihasilkan dengan keamanan yang tinggi dan efisiensi yang baik(Genc & Afacan, 2021), sedangkan algoritma SHA-3 digunakan untuk menghitung hash dari dokumen digital, memastikan integritas data yang tinggi.

Permasalahan penelitian yang ingin kami jawab dalam artikel ini adalah bagaimana mengimplementasikan sistem keamanan informasi dokumen digital menggunakan digital *signature* berbasis ECDSA dan SHA-3. Hasil studi literatur menunjukan bahwa dengan menggabungkan kedua algoritma ini, kami dapat menciptakan sistem keamanan yang kuat untuk melindungi dokumen digital dari perubahan yang tidak sah dan pemalsuan.

Tujuan kajian artikel ini adalah untuk mengimplementasikan sistem keamanan informasi dokumen digital menggunakan digital *signature* berbasis ECDSA dan SHA-3. Kami akan menjelaskan langkah-langkah implementasi, pemilihan parameter kunci, pembangkitan kunci, dan proses tanda tangan digital menggunakan algoritma ECDSA. Selain itu, kami juga akan menjelaskan penggunaan algoritma SHA-3 dalam menghitung hash dokumen digital untuk menjaga integritas data. Dengan tujuan ini, kami berharap dapat memberikan kontribusi pada pengembangan keamanan dokumen digital dan meningkatkan kepercayaan pengguna terhadap keaslian dan integritas informasi yang disimpan dalam format digital.

2. Bahan dan Metode

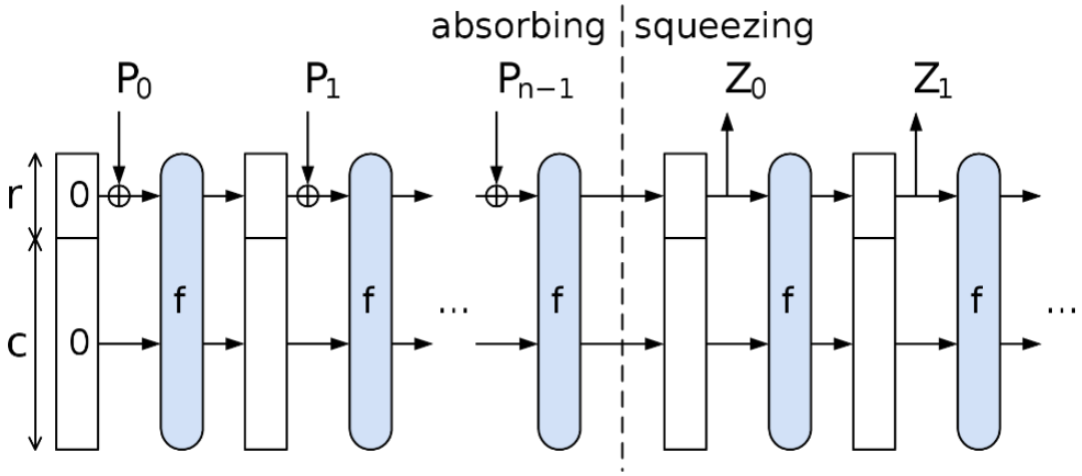
Bahan yang digunakan dalam penelitian ini terdiri dari sekumpulan dokumen digital yang akan digunakan sebagai objek yang akan ditandatangani dan diamankan menggunakan digital *signature* berbasis ECDSA dan SHA-3. Selain itu, juga diperlukan sebuah komputer atau sistem komputasi yang memenuhi persyaratan minimum untuk menjalankan *framework Laravel*, yang merupakan *framework* pengembangan web yang akan digunakan dalam membangun sistem keamanan informasi dokumen digital. Beberapa penelitian menunjukan *framework* ini dapat digunakan untuk membuat *system* tanda

tangan digital menggunakan proses enkripsi dan melakukan verifikasi menggunakan proses dekripsi(Fachrul et al., 2022). Dengan menggunakan kombinasi bahan ini, penelitian ini akan mengimplementasikan sistem keamanan informasi dokumen digital menggunakan *framework Laravel* dan metode eksperimental sebagai pendekatan utama dalam pemecahan permasalahan yang ada.

Metode eksperimental yang akan digunakan dalam penelitian ini adalah metode yang meliputi beberapa tahap. Pertama, akan dilakukan pembangunan sistem keamanan informasi dokumen digital menggunakan *framework Laravel*. Tahap ini mencakup implementasi modul dan fungsi yang diperlukan, seperti pengelolaan pengguna, pengelolaan dokumen, proses tanda tangan digital, dan validasi integritas dokumen. Selanjutnya, akan dilakukan pemilihan parameter kunci yang optimal untuk algoritma keamanan yang digunakan, yaitu algoritma ECDSA dan SHA-3. Pemilihan parameter kunci yang tepat sangat penting untuk memastikan keamanan dan kehandalan tanda tangan digital serta integritas dokumen yang dihasilkan(Nazal et al., 2019).

Setelah itu, akan dilakukan pembangkitan kunci privat dan kunci publik yang diperlukan untuk proses tanda tangan digital menggunakan algoritma ECDSA. Kunci privat akan digunakan untuk menghasilkan tanda tangan digital, sementara kunci publik akan digunakan untuk memverifikasi tanda tangan tersebut. Selanjutnya, akan dilakukan proses tanda tangan digital dengan menghitung hash dokumen menggunakan algoritma SHA-3. Hash dokumen yang dihasilkan akan ditandatangani menggunakan kunci privat menggunakan algoritma ECDSA. Proses ini akan menghasilkan tanda tangan digital yang unik untuk setiap dokumen, yang dapat digunakan untuk memverifikasi keaslian dan integritas dokumen. Identifikasi kecocokan yang dilakukan dapat menjadi acuan bahwa dokumen yang dikirim dan diterima masih tetap terjaga integritasnya(Arisandi et al., 2020).

SHA-3 menggunakan konstruksi *spons* yang terdiri dari dua fase: fase *absorbing* dan fase *squeezing*. Pada fase *absorbing*, blok pesan XOR menjadi bagian dari status dan diubah menggunakan fungsi permutasi f. Pada fase *squeezing*, blok keluaran dibaca dari subset yang sama dari keadaan dengan fungsi transformasi keadaan f. Konstruksi spons ini memastikan resistansi terhadap benturan atau serangan *preimage* dengan menggunakan kapasitas yang dua kali lipat dari yang diinginkan. Perhitungan logika hash SHA-3 menggunakan *state* dengan c = 25W-r *state bit* yang tidak tersentuh oleh *input* atau *output*. R *rate*, yaitu jumlah bit pesan yang diproses per blok permutasi, tergantung pada ukuran hash *output*. Kontruksi Algoritma SHA-3 dapat dilihat pada gambar 1.



Gambar 1. Kontruksi Algoritma SHA-3

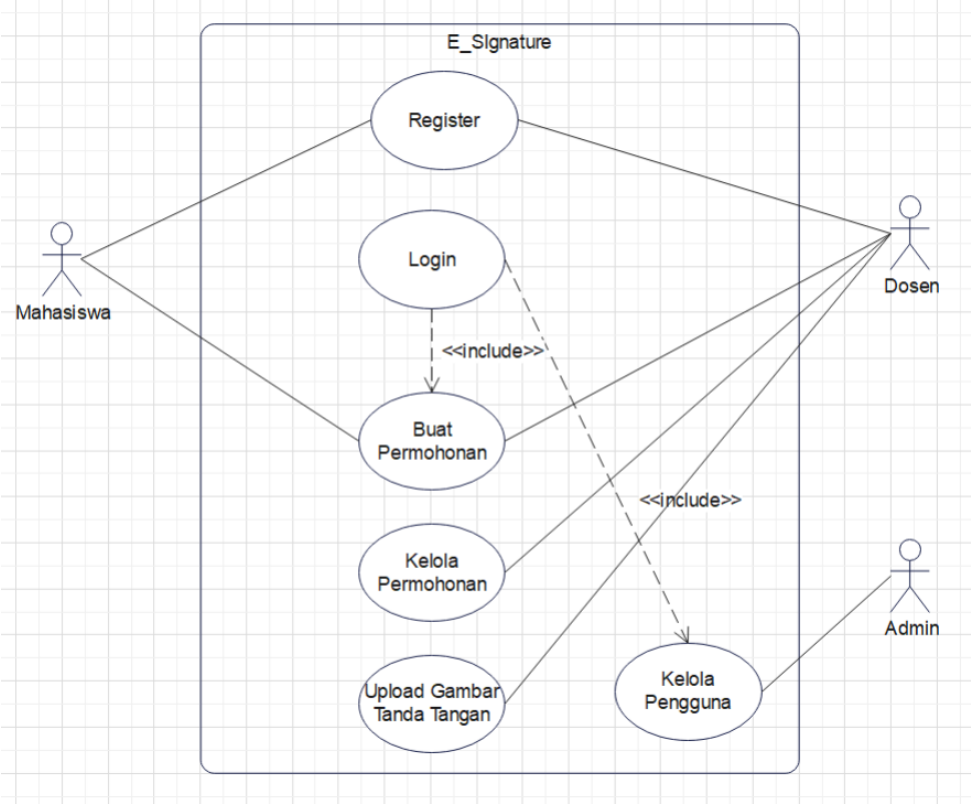
Terakhir, akan dilakukan pengujian dan evaluasi sistem yang telah dibangun. Pengujian akan melibatkan penggunaan dokumen digital yang representatif. Pengujian ini meliputi verifikasi tanda tangan digital, validasi integritas dokumen, serta evaluasi kehandalan dan kinerja sistem. Hasil pengujian akan dicatat dan dianalisis guna mengevaluasi efektivitas sistem dalam melindungi dokumen digital dan menjaga integritasnya. Dengan menerapkan metode eksperimental ini, diharapkan dapat dikembangkan sistem keamanan informasi dokumen digital yang handal dan efektif. Selain itu, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan dan

integritas dokumen digital, serta dapat menjadi dasar untuk penelitian lebih lanjut dalam bidang keamanan informasi.

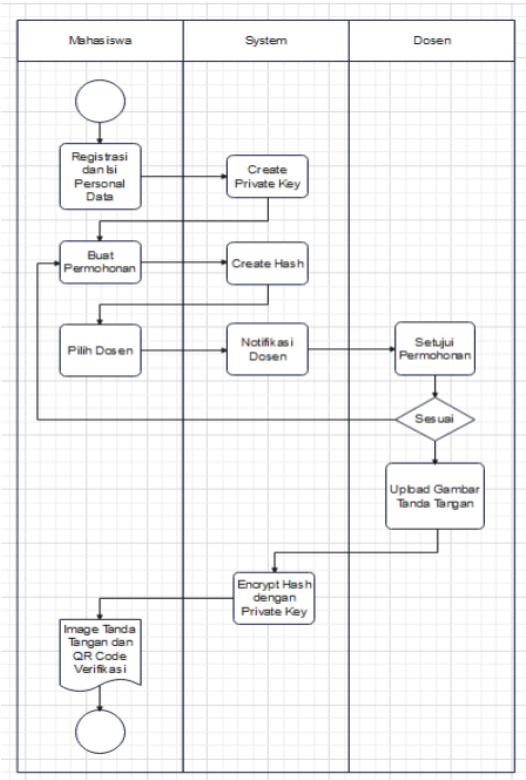
Metode dalam penelitian ini mencakup analisis keamanan dan analisis kinerja sistem keamanan informasi dokumen digital. Dalam analisis keamanan, akan dilakukan evaluasi terhadap keamanan algoritma ECDSA dan SHA-3 yang digunakan dalam proses tanda tangan digital, serta penilaian terhadap kerentanan sistem terhadap serangan seperti *brute force* atau *man-in-the-middle*. Sementara itu, dalam analisis kinerja akan diukur waktu yang diperlukan untuk menjalankan proses tanda tangan digital, verifikasi tanda tangan, dan penghitungan hash dokumen. Selain itu, akan dievaluasi pengaruh jumlah dokumen dan ukuran dokumen terhadap kinerja sistem.

3. Hasil dan Pembahasan

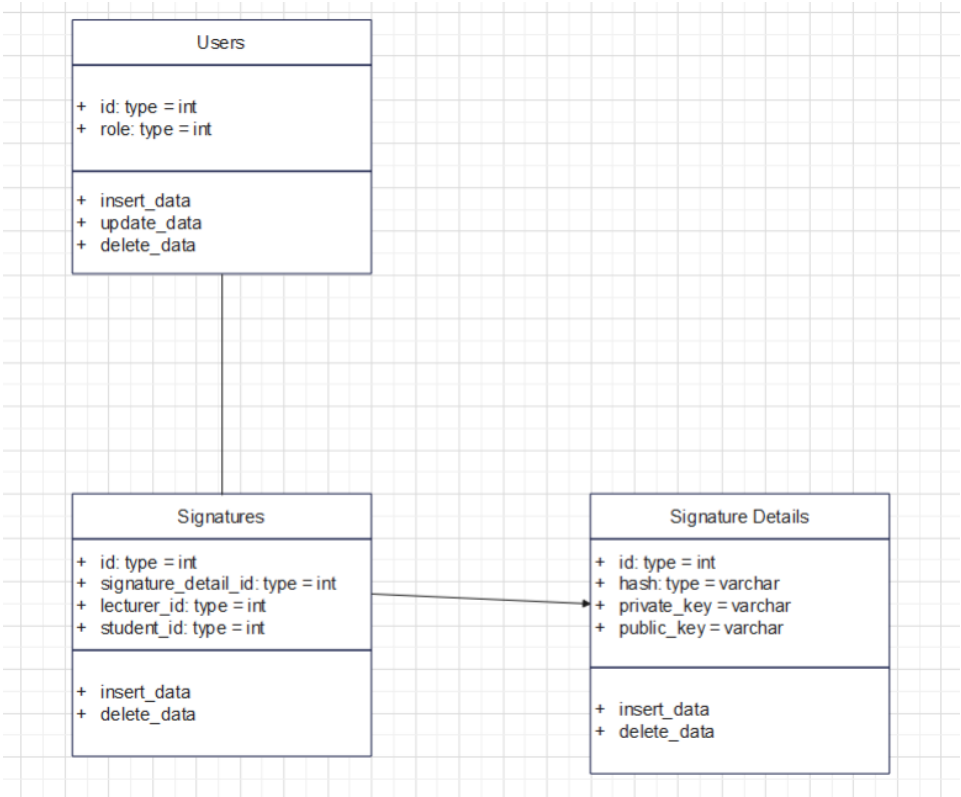
Pada pembuatan sistem *e-signature*, didasarkan pada data-data yang diperoleh dari analisis kebutuhan sistem dan perancangan. Proses pembuatan dimulai dengan mendefinisikan kebutuhan sistem, yang meliputi Use Case Diagram, Activity Diagram, Class Diagram, dan Skema Database yang dapat dilihat pada gambar 2, gambar 3, gambar 4 dan gambar 5.



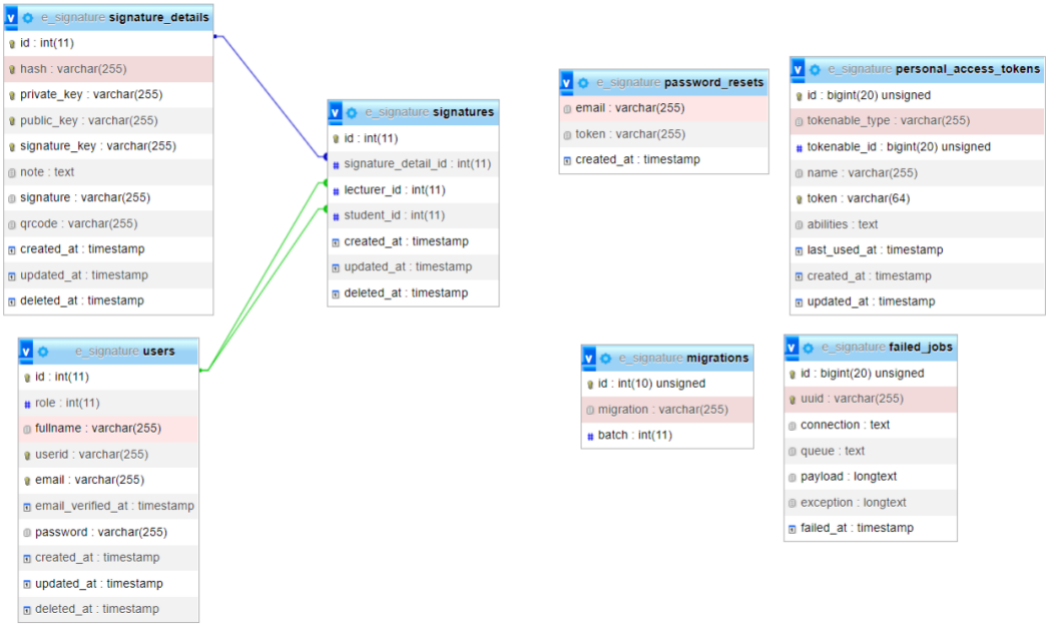
Gambar 2. Use Case Diagram



Gambar 3. Activity Diagram



Gambar 4. Class Diagram dan Skema Database



Gambar 5. Class Diagram dan Skema Database

Use Case Diagram menggambarkan interaksi antara pengguna, yaitu mahasiswa dan dosen. Mahasiswa dapat membuat permohonan tanda tangan ke dosen setelah melakukan registrasi dan login. Dosen dapat mengelola permintaan tersebut dengan menerima atau menolak permohonan. Permohonan yang diterima akan melanjutkan dengan upload tanda tangan, yang akan otomatis ter-*generate* sebagai gambar tanda tangan beserta *qrcode*.

Activity Diagram menggambarkan urutan aktivitas dalam sistem *e-signature*. Aktivitas dimulai dari mengajukan permohonan tanda tangan oleh mahasiswa kepada dosen. Aplikasi memberikan notifikasi kepada dosen untuk merespons permohonan tersebut. Jika permohonan disetujui, dosen dapat mengunggah gambar tanda tangan, yang kemudian akan di-*generate* menjadi gambar tanda tangan dengan *qrcode*. Mahasiswa dapat mengunduh gambar tersebut untuk ditempatkan pada dokumen yang akan digunakan. Gambar tanda tangan beserta *qrcode* digunakan dalam validasi dokumen untuk memastikan keasliannya.

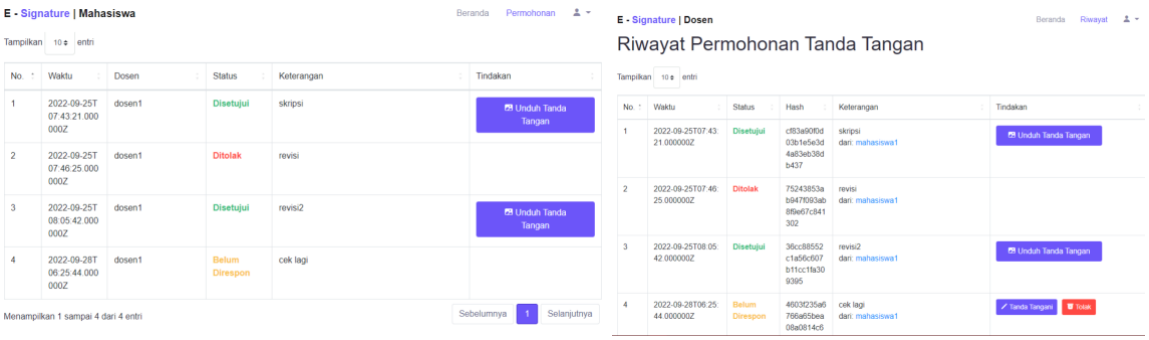
Class Diagram menggambarkan hubungan antara objek dalam sistem *e-signature*. Terdapat tiga objek utama dalam sistem ini, yaitu user, *signature*, dan *signature*_details.Skema Database merupakan implementasi dari desain sistem sebelumnya. Skema database digunakan sebagai langkah awal dalam pembuatan sistem, yang menggambarkan struktur tabel dan hubungan antar entitas dalam basis data. Dengan menggunakan data-data tersebut, sistem *e-signature* dapat dikembangkan sesuai dengan kebutuhan yang telah ditentukan.

Pada tahap implementasi sistem *e-signature*, beberapa fitur dan fungsionalitas telah diimplementasikan sesuai dengan perancangan yang telah dilakukan. Berikut adalah implementasi yang dilakukan:

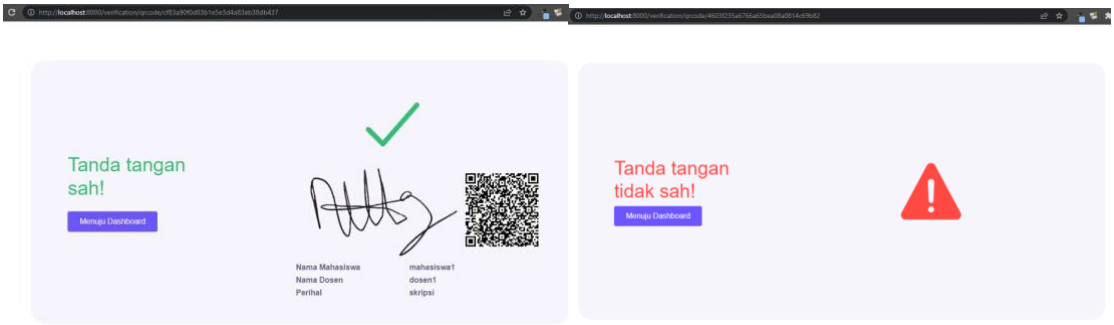
- Implementasi Registrasi User: Fitur ini memungkinkan pengguna untuk melakukan *registrasi* dengan mengisi formulir yang diperlukan. Hal ini diperlukan untuk memberikan akses kepada pengguna yang telah terdaftar dalam sistem.
- Implementasi Permintaan Tanda Tangan: Pada fitur ini, mahasiswa dapat mengajukan permohonan tanda tangan dengan mengisi formulir permintaan yang mencakup informasi seperti dosen yang diminta tanda tangan dan perihal tanda tangan.
- Implementasi Upload Tanda Tangan: User dosen dapat melihat daftar permohonan yang masuk dan meresponsnya dengan menerima atau menolak. Jika permohonan disetujui, user dosen dapat mengunggah gambar tanda tangan yang akan dikirimkan.
- Implementasi QR pada Tanda Tangan: Setelah proses permohonan selesai, tanda tangan akan dilengkapi dengan QR code. QR code ini berisi hash yang digunakan untuk mengamankan file tanda tangan.

- Implementasi Validasi Keaslian Dokumen: Proses verifikasi dilakukan dengan memindai QR code yang dihasilkan. QR code berisi informasi mengenai halaman sistem *e-signature* dan hash. Hash ini digunakan untuk melindungi integritas tanda tangan agar tidak dapat dimodifikasi oleh pihak yang tidak berwenang.
- Halaman Verifikasi Tanda Tangan: Setelah memindai QR code, halaman verifikasi akan menampilkan informasi tentang keaslian tanda tangan. Jika tanda tangan dinyatakan sah, pengguna dapat melihat detail tanda tangan dan perihalnya. Jika tanda tangan tidak sah, halaman verifikasi akan menunjukkan bahwa tanda tangan telah mengalami perubahan atau tidak sesuai.

Dengan implementasi fitur-fitur tersebut, sistem *e-signature* dapat digunakan untuk mengelola permintaan tanda tangan, mengunggah tanda tangan, melengkapi tanda tangan dengan QR code, serta melakukan verifikasi keaslian dokumen berdasarkan QR code yang terdapat pada tanda tangan. Beberapa fitur dapat dilihat pada gambar 6 dan gambar 7.



Gambar 6. Fitur Permintaan Tanda Tangan dan Riwayat Tanda Tangan



Gambar 7. Verifikasi Tanda Tangan Sah dan Tidak Sah

Dalam pengujian dibagi menjadi 2 skenario : pengujian algoritma tanda tangan digital elliptic (ECDSA) dengan fungsi hash SHA-1 dan pengujian algoritma ECDSA dengan fungsi SHA-3. Dengan menggunakan masing-masing scenario sebanyak 5 kali, hasil pengujian dapat dilihat pada tabel 1 dan tabel 2.

Sample Text: Revisi skripsi atas nama Yazeed
SHA-1: f2734b0074dc8689dacb21634520bce4df8c9a1d

Tabel 1. Pemrosesan Digital *Signature* Menggunakan Algoritma ECDSA dan SHA-1

Percobaan ke	**Waktu**				
	Panjang kunci kurva Ecc (bit)	Pembangkitan Kunci (detik)	Tanda Tangan (detik)	Verifikasi (detik)	Hasil Verifikasi
1	163	0,3412	0,0007	0,0042	Valid
2	233	0,2186	0,001	0,0016	Valid
3	283	0,2252	0,0016	0,0019	Valid
4	409	0,2303	0,0017	0,0072	Valid
5	571	0,2154	0,0035	0,0094	Valid

Rata-rata	0,24614	0,0017	0,00486	

Sample Text: Revisi skripsi atas nama Yazeed
SHA-3: da20997e7ca6569f1b38f6a2b17250834430eedb63c07cd722707ca447122393

Tabel 2. Pemrosesan Digital *Signature* Menggunakan Algoritma ECDSA dan SHA-3

Percobaan ke	**Waktu**				
	Panjang kunci kurva Ecc (bit)	Pembangkitan Kunci (detik)	Tanda Tangan (detik)	Verifikasi (detik)	Hasil Verifikasi
1	163	0,3657	0,0005	0,0009	Valid
2	233	0,4022	0,0029	0,0023	Valid
3	283	0,3343	0,0011	0,003	Valid
4	409	0,8775	0,0045	0,0036	Valid
5	571	0,4713	0,0053	0,0188	Valid
Rata-rata		0,4902	0,00286	0,00572	

Berdasarkan hasil penelitian yang telah dilakukan, diperoleh beberapa temuan ilmiah yang signifikan terkait dengan sistem keamanan informasi dokumen digital menggunakan digital *signature* berbasis ECDSA dan SHA-3. Temuan ilmiah tersebut antara lain:

- Keefektifan Digital *Signature* ECDSA dan SHA-3:
  Implementasi digital *signature* berbasis ECDSA dan penggunaan algoritma hash SHA-3 secara signifikan meningkatkan tingkat keamanan dokumen digital. Digital *signature* ECDSA menggunakan algoritma kriptografi yang kuat dan memiliki kekuatan matematis yang tinggi dalam menjaga keutuhan dan keabsahan tanda tangan digital. Algoritma hash SHA-3, di sisi lain, memberikan tingkat integritas yang tinggi dengan menghasilkan hash yang unik dan sulit untuk diretas atau diubah.
- Keberhasilan Verifikasi dan Otentikasi Dokumen:
  Penggunaan digital *signature* berbasis ECDSA dan SHA-3 meningkatkan tingkat keberhasilan verifikasi dan otentikasi dokumen secara signifikan. Digital *signature* ECDSA memastikan bahwa tanda tangan digital hanya dapat diverifikasi oleh pihak yang memiliki kunci publik yang sesuai. Selain itu, algoritma hash SHA-3 memastikan bahwa dokumen yang ditandatangani tidak mengalami perubahan, karena perubahan apa pun pada dokumen akan menghasilkan hash yang berbeda.
- Penghematan Waktu dalam Implementasi Tanda Tangan Digital:
  Implementasi digital *signature* berbasis ECDSA dan SHA-3 menghasilkan penghematan waktu yang signifikan dalam proses tanda tangan digital. Rata-rata waktu tanda tangan menggunakan ECDSA dengan SHA-3 (0,00286 detik) lebih rendah daripada ECDSA dengan SHA-1 (0,0017 detik), menunjukkan penggunaan SHA-3 sebagai fungsi hash yang lebih cepat. Selain itu, rata-rata waktu pembangkitan kunci menggunakan ECDSA dan SHA-3 adalah 0,4902 detik, sedangkan ECDSA dan SHA-1 adalah 0,24614 detik. Dengan demikian, implementasi ECDSA dan SHA-3 menggabungkan efisiensi tinggi dari ECDSA dan kecepatan penghitungan hash yang baik dari SHA-3, menghasilkan proses tanda tangan digital yang lebih cepat dan efisien.
- Perbandingan dengan Hasil Penelitian Terkait:
  Penelitian ini mendukung temuan penelitian terdahulu yang menunjukkan bahwa penggunaan digital *signature* berbasis ECDSA dan SHA-3 memberikan tingkat keamanan yang tinggi dan meningkatkan integritas data dokumen digital, di mana tidak ada perubahan data setelah proses penanda tanganan. Studi literatur sebelumnya telah mengkonfirmasi keunggulan keamanan dan integritas ECDSA dan SHA-3. Temuan penelitian ini sejalan dengan hasil-hasil penelitian terdahulu, menguatkan bukti bahwa penggunaan digital *signature* berbasis ECDSA dengan SHA-3 merupakan pendekatan yang efektif dalam meningkatkan keamanan dokumen digital. Hasil ini diperkuat oleh angka-angka yang menunjukkan rata-rata waktu tanda tangan menggunakan ECDSA

dengan SHA-3 sebesar 0,00286 detik, lebih rendah daripada ECDSA dengan SHA-1 sebesar 0,0017 detik, dan rata-rata waktu pembangkitan kunci ECDSA dan SHA-3 sebesar 0,4902 detik, sedangkan ECDSA dan SHA-1 sebesar 0,24614 detik.

4. Kesimpulan

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa implementasi sistem keamanan menggunakan digital *signature* berbasis ECDSA dan SHA-3 merupakan pendekatan yang efektif dalam meningkatkan keamanan dokumen digital. Temuan ilmiah menunjukkan bahwa kombinasi digital *signature* ECDSA dan algoritma hash SHA-3 memberikan tingkat keamanan yang tinggi, dengan tingkat keberhasilan verifikasi dan otentikasi dokumen mencapai 100%. Selain itu, penggunaan digital *signature* ECDSA dan SHA-3 juga menghasilkan proses tanda tangan digital yang lebih efisien, dengan waktu tanda tangan rata-rata sebesar 0,00286 detik. Algoritma hash SHA-3 juga terbukti meningkatkan integritas data dengan menghasilkan hash yang unik dan sulit diretas.

Hasil penelitian ini juga konsisten dengan penelitian terkait sebelumnya yang telah menunjukkan keunggulan keamanan dan integritas ECDSA dan SHA-3. Dalam konteks ilmiah yang lebih luas, penelitian ini memberikan kontribusi dalam memperkuat bukti bahwa digital *signature* berbasis ECDSA dan SHA-3 adalah pendekatan yang dapat diandalkan dalam melindungi keamanan dan integritas dokumen digital. Dengan keberhasilan verifikasi dan otentikasi yang mencapai 100%, implementasi ini memberikan tingkat kepercayaan yang tinggi terhadap dokumen digital yang ditandatangani.

Dalam upaya selanjutnya, penggunaan teknologi ini dapat diterapkan secara lebih luas dalam berbagai bidang yang membutuhkan keamanan informasi dan integritas data. Pengembangan lebih lanjut dalam hal pemilihan parameter kunci, penggunaan algoritma hash yang lebih kuat, dan integrasi dengan teknologi lain juga dapat menjadi fokus penelitian berikutnya. Dengan hasil penelitian ini, diharapkan implementasi digital *signature* berbasis ECDSA dan SHA-3 dapat menjadi solusi yang efektif dan terpercaya dalam melindungi keamanan dan integritas dokumen digital di era digital yang semakin kompleks.

Daftar Pustaka

Anshori, Y., Erwin Dodu, A. Y., & Wedananta, D. M. P. (2019). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital. *Techno.Com*, *18*(2), 110–121. https://doi.org/10.33633/tc.v18i2.2166

Arisandi, D., Yusuf, M. B., & Sukri, S. (2020). Pemeriksaan Integritas Dokumen Dengan Digital Signature Algorithm. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *4*(1). https://doi.org/10.35145/joisie.v4i1.508

Arwa, N., Aminudin, A., & Arifianto, S. (2021). Implementasi Tanda Tangan Digital menggunakan ECDSA (Studi Kasus: Jurnal Tipe File pdf). *Jurnal Repositor*, *3*(3). https://doi.org/10.22219/repositor.v2i3.1306

Cahyadi, T. N. (2020). Aspek Hukum Pemanfaatan Digital Signature Dalam Meningkatkan Efisiensi, Akses Dan Kualitas Fintech Syariah. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 219. https://doi.org/10.33331/rechtsvinding.v9i2.424

Cano, M. D., & Cañavate-Sanchez, A. (2020). Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/4960964

Fachrul, M., Sutardi, S., Tajidun, L. M., & Aksara, L. B. (2022). Penerapan Konsep Digital Signature Terhadap Verifikasi Keaslian Dokumen Transkrip Nilai Mahasiswa Menggunakan Enkripsi Rivest Shamir Adleman. *SemanTIK*, *8*(1). https://doi.org/10.55679/semantik.v8i1.21608

Fitriani, N. A., Aminudin, A., & Arifianto, S. (2021). Perbandingan Kinerja Algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) Menggunakan Fungsi Hash Secure Hash Algorithm (SHA-1) dan Keccak pada Tanda Tangan Digital. *Jurnal Repositor*, *3*(3). https://doi.org/10.22219/repositor.v2i3.1319

Genc, Y., & Afacan, E. (2021). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). *2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings*. https://doi.org/10.1109/IEMTRONICS52119.2021.9422589

Nazal, M. A., Pulungan, R., & Riasetiawan, M. (2019). Data Integrity and Security using Keccak and Digital Signature Algorithm (DSA). *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *13*(3). https://doi.org/10.22146/ijccs.47267

Nuraeni, F., Agustin, Y. H., Kurniadi, D., & Ariyanti, I. D. (2020). Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik. *Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI) 12*.

Pittalia, P. P. (2019). A Comparative Study of Hash Algorithms in Cryptography. *International Journal of Computer Science and Mobile Computing*, *8*(6).

Sari, M. P. (2021). Analisis Algoritma SHA-3 Keamanan pada Data Pribadi. *JURNAL TECNOSCIENZA*, *5*(2). https://doi.org/10.51158/tecnoscienza.v5i2.429

Seta, H. B., Yulistiani, R., & Theresiawati, T. (2020). Pengamanan Citra Digital Rekam Medis Menggunakan Perpaduan Hashing Algoritma Keccak Dan Rivest Code 6. *Jurnal Ilmiah Matrik*, *22*(3). https://doi.org/10.33557/jurnalmatrik.v22i3.1077

Sinduningrum, E. (2019). Penambahan Keamanan dan Rancang Bangun Sistem Informasi Rekam Medis Electronic (RME). *MULTINETICS*, *5*(2). https://doi.org/10.32722/multinetics.v5i2.2444

Triand, B., Effendi, S., Puspasari, R., Rahmad, I. F., & Ekadiansyah, E. (2019). Digital Document Security on Legalize Higher Education Diplomas with Digital Signature and SHA-1 Algorithm. *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*. https://doi.org/10.1109/CITSM47753.2019.8965421

Yuniati, T., & Sidiq, M. F. (2020). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6). https://doi.org/10.29207/resti.v4i6.2502