(2024), 2 (4): 131–149 **Scientica** 2985-5624
Jurnal Ilmiah Sain dan Teknologi

PENERAPAN DIGITAL SIGNATURE UNTUK PERSURATAN DENGAN MENGGUNAKAN METODE ALGORITMA SHA-1 DI SEKTOR PERTANIAN, KETAHANAN PANGAN DAN PERIKANAN KAB.MEMPAWAH

Helfi Nasution[1)], Heri Priyanto[2)], Nanda Widya[3)]
Program Studi Sarjana Informatika Fakultas Teknik Informatika , Universitas Tanjungpura, Pontianak
Email : ndaawidya11@gmail.com, nandawidya@student.untan.ac.id

Abstract (English)
A digital signature is a value that depends on cryptography on the message and the sender of the message using the sha-1 algorithm. Sha-1 is an algorithm used to verify data authenticity. Problems that often occur in sending using digital media are important documents that should maintain their authenticity, but usually the documents that reach the recipient are documents that have been modified, therefore of course digital signature This is made for document security so that the recipient of the document has been affixed digital signature sure that the documents received are original without modification. The steps for creating a digital signature are by creating a key from the document and verifying the validity of the signature. By collecting data from observations and interviews as well as literature studies and system design using Unified Modeling Language (UML) then based on testingWhite Box Testing. Users who want to send a document, the system will encrypt the text of the document .

Article History
Submitted: 9 Januari 2024
Accepted: 19 Januari 2024
Published: 20 Januari 2024

Key Words
Digital signature, Cryptography,sha-1 algorithm, Encryption.

Abstrak (Indonesia)
Digital signature merupakan nilai yang bergantung dari sebuah kriptografi pada pesan dan pengirim pesan dengan menggunakan algoritma sha-1. Sha-1 merupakan algoritma yang digunakan untuk memverifikasi keaslian data. Masalah yang sering terjadi dalam pengiriman menggunakan media digital dokumen penting yang seharusnya tetap terjaga keasliannya malah biasanya dokumen yang sampai ke penerima adalah dokumen yang telah termodifikasi maka dari itu tentunya *digital signature* ini dibuat untuk keamanan dokumen supaya penerima dokumen yang telah dibubuhi *digital signature* yakin bahwa dokumen yang diterima masih asli tanpa termodifikasi. langkah pembuatan digital signature yaitu dengan pembuatan kunci dari dokumen dan memverifikasi keabsahan tanda tangan. Dengan pengumpulan data dari observasi dan wawancara serta studi literatur serta perancangan sistem dengan menggunakan *Unified Modeling Language* (UML) lalu berdasarkan dari pengujian *White Box Testing*. Pengguna yang ingin mengirimkan dokumen maka sistem akan melakukan enkripsi dari teks dokumen tersebut.

Sejarah Artikel
Submitted: 9 Januari 2024
Accepted: 19 Januari 2024
Published: 20 Januari 2024

Kata Kunci
Digital signature, Kriftografi, Algoritma sha-1, Enkripsi.

Pendahuluan

Pengamanan dokumen dengan kriftografi dipakai mengatasi keaslian dokumen untuk diterapkan di penerapan digital signature pada persuratan di Sektor Pertanian, Ketahanan Pangan Dan Perikanan Kab.Mempawah ini dibuat untuk mengamankan dokumen dengan tanda tangan dengan pengamanan yang lebih baik untuk menghindari kecurangan dalam pemalsuan data atau perubahan dari data dokumen tersebut.

Sektor Pertanian, Ketahanan Pangan Dan Perikanan Kab.Mempawah adalah sebuah badan yang bergerak di bidang pertanian yang ingin meningkatkan sistem pengolahan data khususnya di keamanan data. Namun demikian untuk pengolahan persuratan masih menggunakan

cara lama dalam pelaksaannya yaitu cara penanda tanganan manual. Dimana tanda tangan adalah alat untuk memvalidasi suatu kesepakatan dan ini sangat penting dilakukan keamanan. Keamanan kriftografi yang di buat ini menggunakan salah satu fungsi dari beberapa hash kriftografi yaitu algoritma sha-1. Algoritma sha-1 ini menggunakan kriptografi block cipher dengan masukkan 64bit blok data dan menghasilkan nilai hash dengan panjang 160 bit.

Proses pembuatan digital signature untuk proses ini ada 2 proses yang diperlukan yaitu digital signature dengan verifikasi dimulai dengan mengubah dokumen menggunakan kriftografi memakai algoritma sha-1 untuk pembentukan message digest dan mengenkripsinya dengan algoritma tersebut menggunakan kunci publik.

Berdasarkankan uraian diatas peneliti bermaksud untuk merancang dan membangun Aplikasi Penerapan Digital Signature Untuk Persuratan dengan Menggunakan Algoritma SHA-1 Di Sektor Pertanian, Ketahanan Pangan Dan Perikanan KAB.Mempawah. Dimana Sektor Pertanian, Ketahanan Pangan Dan Perikanan KAB.Mempawah adalah instansi yang membutuhkan aplikasi Digital signature untuk menjaga keabsahan dokumen. Aplikasi digital signature yang akan dibangun akan berjalan sesuai kebutuhan pada Sektor Pertanian, Ketahanan Pangan Dan Perikanan KAB.Mempawah.

Metode Penelitian

Metode penelitian yang akan dilakukan dengan penelitian ini angara lain :

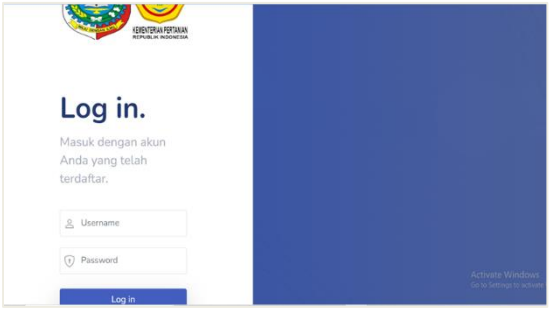
1. Pengumpulan Data
   Pada tahap ini peneliti melakukan pengumpulan data untuk mempermudah melakukan tahap selanjutnya yaitu tahap analisis memalui berbagai cari meliputi: wawancara dan studi literatur yang berkaitan dengan penerapan digital signature menggunakan algoritma SHA pada dokumen seperti konsep digital signature, cara kerja Algoritma SHA pada digital signature, fungsi hash satu arah SHA dan implementasi digital signature pada bahasa pemograman.
2. Analisis
   Setelah melakukan tahap pengumpulan data maka yang dilakukan selanjutnya adalah melakukan proses Analisis. Adapun proses analisis yang dilakukan untuk menganalisa bagian proses aplikasi yang akan dibangun agar sesuai dengan proses yang berjalan pada Di Sektor Pertanian, Ketahanan Pangan Dan Perikanan KAB.Mempawah.
3. Perancangan
   Tahap ini merupakan tahap perancangan aplikasi pada tahap ini akan dilakukan proses pembuatan rancangan aplikasi meliputi perancangan antarmuka aplikasi dan perancangan digital signature berdasarkan kebutuhan untuk mengimplementasikan digital signature menggunakan algoritma SHA.
4. Implementasi dan Pengujian
   Tahap ini merupakan tahap dimana aplikasi yang dibuat siap untuk diimplementasikan pada 1 Di Sektor Pertanian, Ketahanan Pangan Dan Perikanan KAB.Mempawah dan dilakukan pengujian.
5. Kesimpulan
   Penarikan kesimpulan merupakan tahap akhir dari penelitian ini. Pada tahap ini dilakukan penulisan laporan berdasarkan hasil penelitian yang telah dilakukan sebelumnya. Laporan hasil penelitian ini kemudian akan digunakan sebagai dokumentasi terhadap penelitian yang telah dilakukan.

Hasil dan Analisis

1. Hasil Implementasi

Sistem yang telah dibangun adalah sebuah *website* yang bersifat responsif, sehingga memungkinkan website ini untuk dapat menyesuaikan dengan perangkat PC/Laptop, Tablet, atau *smartphone*. Berikut ini adalah penjelasan sistem yang telah dibangun.

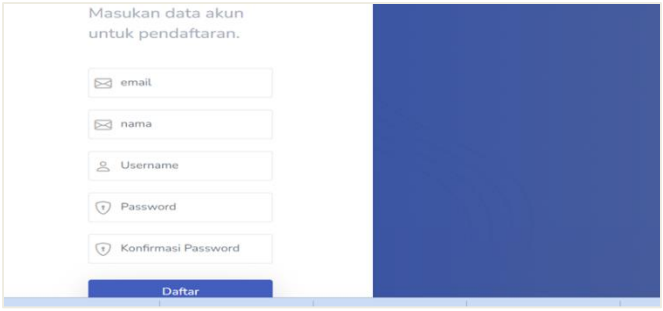
2. Halaman Antarmuka Login



Gambar 4.1 Halaman Antarmuka *Login*

Pada halaman *login* terdapat dua kolom yaitu kolom untuk masukkan *username* dan kolom *password*, selain itu di halaman *login* juga ada tombol untuk registrasi ini berfungsi sebagai registrasi awal utuk bisa diberikan akses dalam aplikasi ini yang dikhusus kan sebagai *user*.

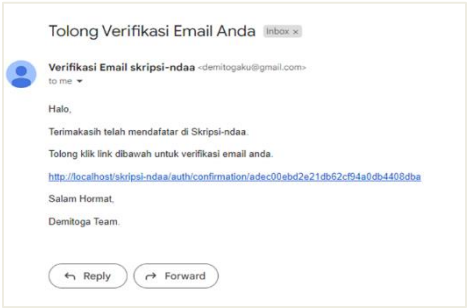
3. Halaman Antarmuka Registrasi



Gambar 4.2 Halaman Antarmuka Registrasi

Halaman registrasi ini hanya untuk *user* yang baru ingin mengakses aplikasi dan user menginputkan sesuai perintah. Admin akan memverifikasi *user* agar dapat masuk ke aplikasi dari aplikasi jika telah diverifikasi registrasi *user* akan mendapatkan *email* dari aplikasi untuk dapat mengakses aplikasi.

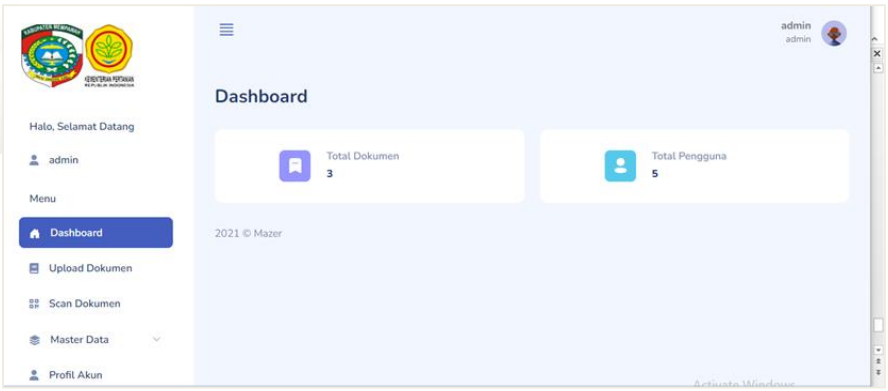
4. Verifikasi *Email User*



Gambar 4.3 Verifikasi *Email* Untuk Masuk Aplikasi

Email verifikasi akan mauk ke *user* setelah amin memverifikasi *user* di aplikasi.

5. Halaman Antarmuka Dashboard Admin

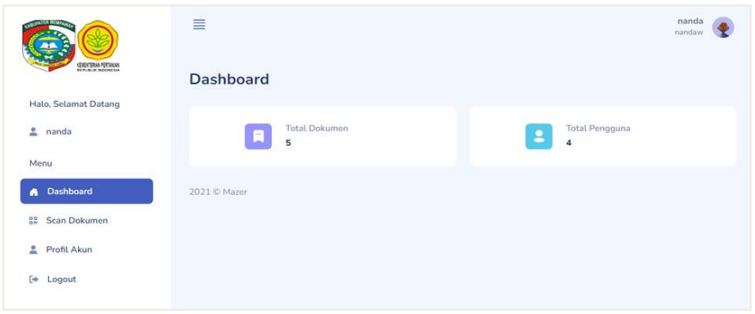


Gambar 4.4 Halaman Antarmuka *Dashboard* Admin

Untuk halaman dashboard admin ad banyak menu yang hanya bisa di lihat oleh admin dengan menu dari gambar tersebut, ini dibuat supaya user tidak bisa megakses data yang ada di aplikasi, fungsi dari menu dashboar admin ialah :

- Upload dokumen: ini menginputkan judul surat,nama penanda tangan dan tanda tangan asli
- Scan dokumen: untuk mengscan barcode dari tanda tangan yang telah di enkripsikan yang dilampirkan ke qrcode
- Master Data: menyimpan data surat dengan tanda tangan yang telah dibuat menjadi digital signature,data pengguna yang bisa mengakses aplikasi tersebut.

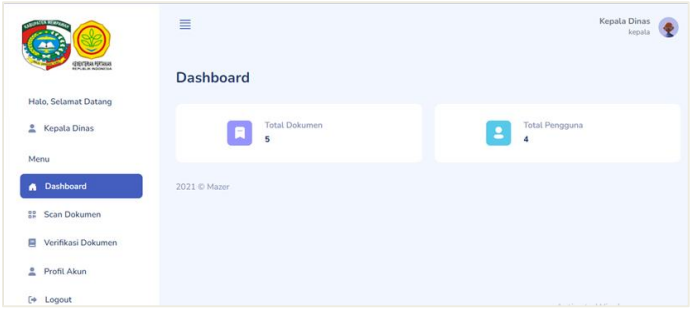
6. Halaman Antarmuka *Dashboard* User



Gambar 4.5 Halaman Antarmuka *Dashboard User*

Halaman *dashboard user* hanya dengan tampilan scan dokumen, profil akun, dan *log out* karena disini *user* hanya bisa mengscan *qrcode* yang telah dikirim oleh aplikasi untuk menerima surat dengan Digital Signature.

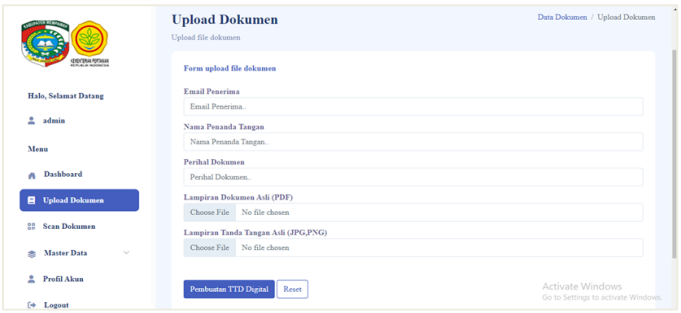
7. Halaman Antarmuka *Dashboard* Kepala Dinas



Gambar 4.6 Halaman Antarmuka Kepala Dinas

Untuk halaman *dashboard* kepala dinas ini dapat memverifikasi dokumen yang telah di *upload* untuk menjadi digital signature dengan mengenkripsikan *file* dokumen.

8. Halaman Antarmuka *Upload* Dokumen



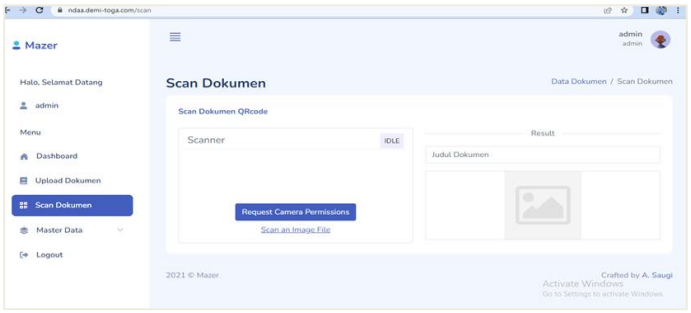
Gambar 4.7 Halaman Antarmuka *Upload* Dokumen

Halaman *upload* dokumen yang dibuat di aplikasi ini dengan inputan yaitu:

- *file* dokumen
- judul dokumen
- lampiran dokumen asli
- lampiran tanda tangan asli.

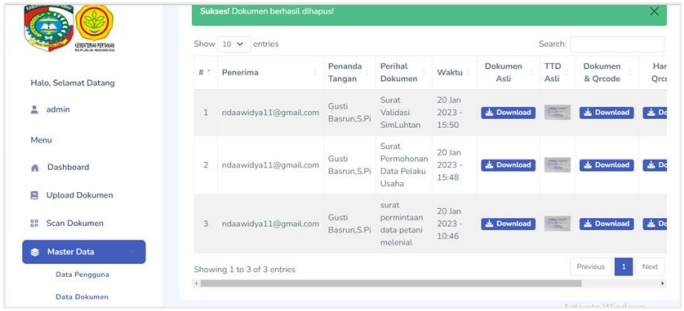
Dengan inputan diatas dibuat untuk mengenkripsi data yang akan dibuatkan tanda tangan digital.

9. Halaman Antarmuka *Scan* Dokumen



Gambar 4.8 Halaman Antarmuka *Scan* Dokumen

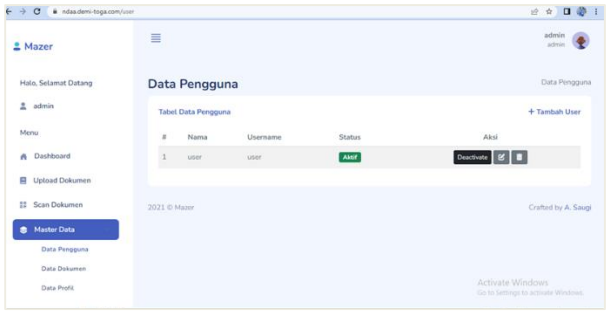
10. Halaman Antarmuka Master Data



Gambar 4.9 Halaman jm Antarmuka Master Data

Halaman master data ini dokumen yang telah di inputkan tersimpan, dan untuk master data ini hanya admin yang bisa memproses dokumen tersebut.

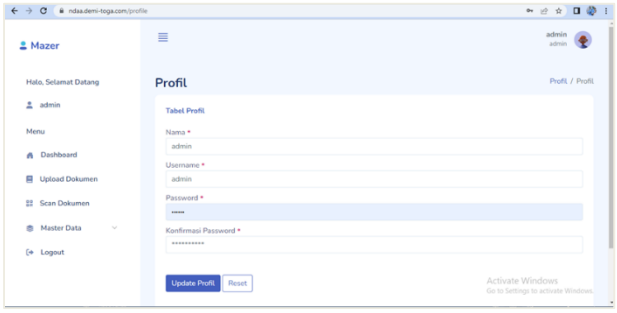
11. Halaman Antarmuka Data *User*



Gambar 4.10 Halaman Antarmuka Data Pengguna

Halaman data pengguna ini tempat data user yang bisa mengakses aplikasi tersimpan.

12. Halaman Antarmuka Data Profil Admin



Gambar 4.11 Halaman Antarmuka Data Profil

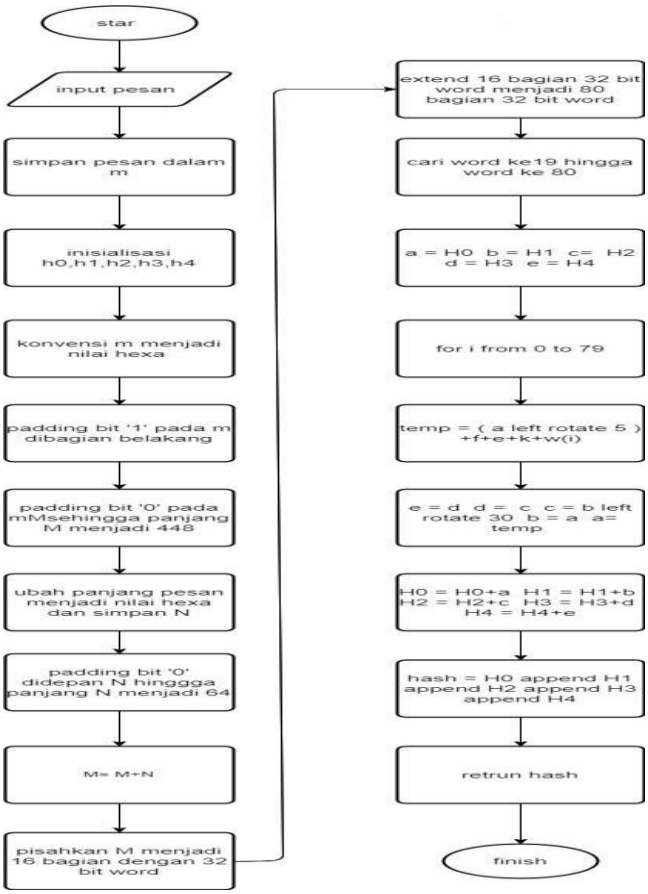
Halaman data profil ini adalah penyimpanan data admin yang bisa diubah *username* dan *password*nya.

13. Hasil Pengujian

Pengujian dilakukan dengan algoritma sha-1 dengan penyandingan metode white box dengan analisis pengujian white box yang mencakup perencanaan dan hasil pengujian.

14. *Flowhart* Algoritma SHA-1

Flowchart bagian ini di jelaskan proses hashing yang dilakukan oleh sha -1 dalam perhitungan.

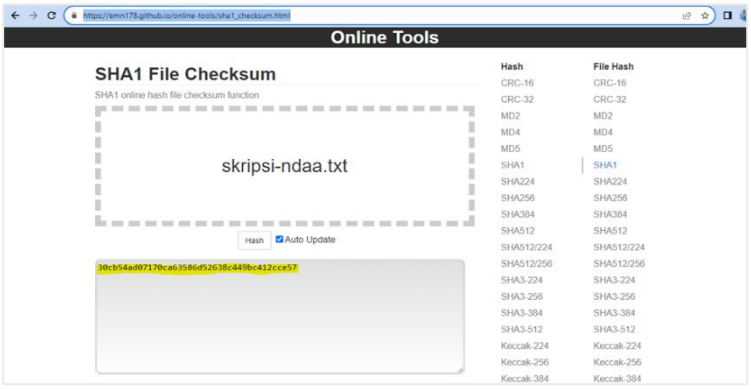


Gambar 4.12 flowchart algoritma sha-1 (Dewa Fakha Shiva, Muhammad Ainur Rony, 2018)

Proses Perhitungan Algoritma SHA-1 *Online*

Perhitungan menggunakan media online dengan inputan yang sama yaitu skripsi-ndaa menggunakan link:

https://emn178.github.io/online-tools/sha1_checksum.html



Gambar 4.12 Proses Perhitungan SHA-1 *Online*

Inputan yang diinputkan didalam tools tersebut adalah inputan yang sama dengan inputan dalam aplikasi dengan hasil nilai yang sama.

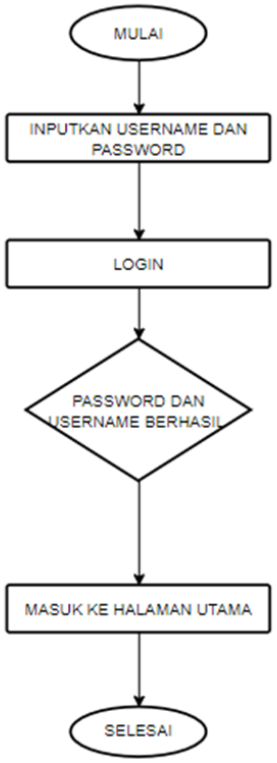
Hasil Pengujian *White Box*

Pengujian sistem dilakukan untuk mengetahui hasil implementasi yang telah dilakukan telah sesuai dengan harapan atau sebaliknya. Pengujian sistem juga bertujuan untuk meminimalisir tarjadinya kesalahan atau error dan bug pada sistem aplikasi. Sistem yang tidak sesuai dengan harapan dapat dikatakan sebagai bug. Untuk itu pengujian sistem menjadi acuan dalam melakukan implementasi. Berikut beberapa pengujian sistem yang silakukan terhadap Aplikasi Penerapan Digital Signature ini.

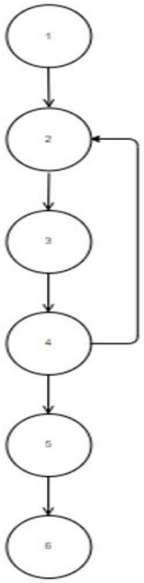
Pengujian dilakukan pada 3 menu utama yang terdapat pada fitur aplikasi Tahapan-tahapan pengujian dimulai dari pembuatan flowchart, pembuatan flow graph. Perhitungan kompleksitas siklomatis, perhitungan jalur independen, dan *test case*.

Proses Login

Login merupakan suatu hal penting dalam sistem aplikasi untuk melakukan akses masuk ke dalam aplikasi agar setiap user/pengguna dapat login ke aplikasi, sehingga hanya orang yang diberikan akses masuk ke aplikasi saja yang dapat mengakses aplikasi tersebut. Dibawah ini adalah flowchart login sebagai berikut:



Gambar 4.13 *Flowchart Login*



Gambar 4.14 *Flow Graph Login* (Dwi Suprapti, Made Kamisutara, Putu Artaya,2017)

Kompleksitas siklomatis pada Gambar 4.17 flow graph login kompleksitas siklomatis dihitung menggunakan 3 (tiga) cara, yaitu :

1. Grafik alir mempunyai 2 region
2. V(G) = 6 edge – 6 node + 2 = 2
3. V(G) = 1 simpul yang diperkirakan + 1 = 2 Dengan demikian kompleksitas siklomatis dari flow graph yang dijelaskan pada Gambar 4.17 adalah 2. Dengan jalur independennya adalah :

Jalur 1 : 1-2-3-4-5-6
Jalur 2 : 1-2-3-4-2-3-5-6

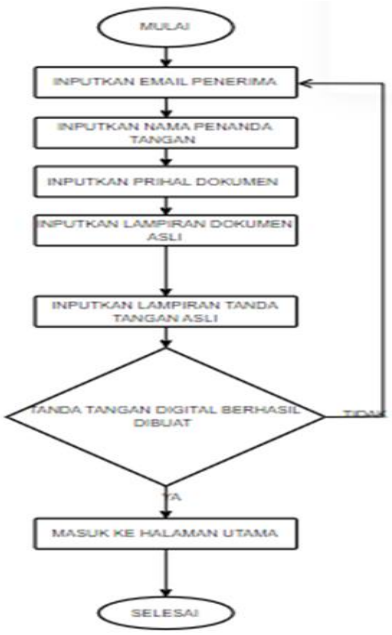
Tabel 4.1 *Test Case*

Path	1
Jalur	1-2-3-4-5
	1.mulai 2. Masukkan username dan password 3.Klik login 4. Validasi data benar 5.Sistem menampilkan halaman utama 6.selesai
Hasil pengujian	Berhasil
Path	2

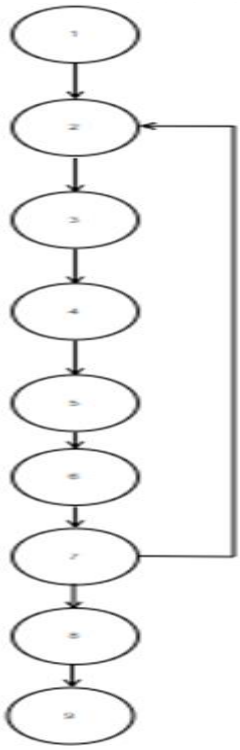
Jalur	1-2-3-4-2-3-5-6
Skenario	1.mulai 2. Masukkan username dan password 3. Klik login 4. Validasi data salah 2. Muncul pesan error. Masukkan kembali username dan password 3. Klik login 5. Sistem menampilkan halaman utama 6. Selesai
Hasil pengujian	Berhasil

Proses *Upload* Dokumen

Upload dokumen digunakan untuk menginputkan data yang akan dibuat menjadi digital signature. Dibawah ini adalah *flowchart upload* dokumen sebagai berikut



Gambar 4.15 *Flowchart Upload* Dokumen



Gambar 4.16 *Flow Graph Upload* Dokumen

Kompleksitas siklomatis pada Gambar 4.25 flow graph daftar item kompleksitas siklomatis dihitung menggunakan 3 (tiga) cara, yaitu :

1. Grafik alir mempunyai 2 region
2. V(G) = 9 edge – 9 node + 2 = 2
3. V(G) = 2 simpul yang diperkirakan + 1 = 3 Dengan demikian kompleksitas siklomatis dari flow graph yang dijelaskan pada Gambar 4.19 adalah 2 Dengan jalur independennya adalah :

Jalur 1 : 1-2-3-4-5-6-7-8-9
Jalur 2 : 1-2-3-4-5-6-7-2-3-4-5-6-8-9

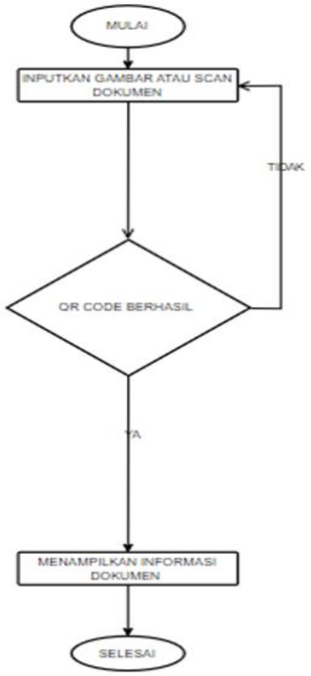
Tabel 4.2 *Test Case*

Path	1
Jalur	1-2-3-4-5-6-7-8-9
Skenario	1.mulai 2.inputkan email penerima 3.inputkan nama penanda tangan 4.inputkan prihal dokumen 5.inputkan lampiran doikumen asli 6.inputkan tanda tangan asli 7.validasi pembuatan tanda tangan digital 8. data tersimpan ke master data 9.selesai
Hasil pengujian	Berhasil
Path	2
Jalur	1-2-3-4-5-6-7-2-3-4-5-6-8-9

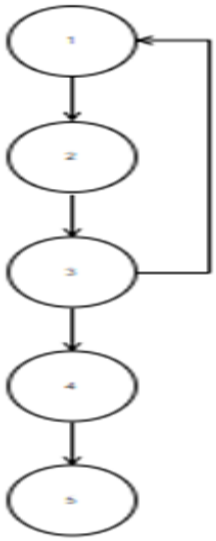
Skenario	1.mulai 2.inputkan email penerima 3.inputkan nama penanda tangan 4.inputkan prihal dokumen 5.inputkan lampiran doikumen asli 6.inputkan tanda tangan asli 7.validasi jika inputan yang dimasukkan salah 2.mengisi ulang inputan email penerima 3. mengisi ulang inputan nama penanda tangan 4.mengisi ulang inputan prihal dokumen 5.mengisi ulang inputan prihal dokumen 6.mengisi ulang inputan tanda tangan asli 8.data tersimpan ke master data 9.selesai
Hasil pengujian	Berhasil

Proses *Scan* Dokumen

Scan dokumen ini menampilkan hasil enkripsi dari dokumen yang telah di inputkan menjadi *qr code* lalu digunakan untuk menampilkan hasil dari inputan *qr code* yang diinputkan. Dibawah ini adalah *flowchart scan* dokumen sebagai berikut:



Gambar 4.17 *Flow Graph Upload* Dokumen



Gambar 4.18 *Flow Graph Scan* Dokumen (Dwi Suprapti, Made Kamisutara, Putu Artaya,2017)
Kompleksitas siklomatis pada Gambar 4.27 *flow graph* daftar item kompleksitas siklomatis dihitung menggunakan 3 (tiga) cara, yaitu :
1. Grafik alir mempunyai 2 region
2. V(G) = 5 edge – 5 node + 2 = 2
3. V(G) = 2 simpul yang diperkirakan + 1 = 3 Dengan demikian kompleksitas siklomatis dari *flow graph* yang dijelaskan pada Gambar 4.27 adalah 2 Dengan jalur independennya adalah :
Jalur 1 : 1-2-3-4-5
Jalur 2 : 1-2-3-2-4-5

Tabel 4.3 *Test Case*

Path	1
Jalur	1-2-3-4-5
Skenario	1.mulai 2.menginputkan gambar qr code gambar atau scan qr code 3.qr code berhasil diproses 4.hasil qr code menampilkan informasi dokumen 5.selesai
Hasil pengujian	Berhasil
Path	2
Jalur	1-2-3-2-4-5

Skenario	1.mulai 2.menginputakan gambar qr code atau scan qr code 3.qr code yang di masukkan tidak dapat diproses 2.menginputkan kembali qr code atau gambar qr code 4.hasil qr code menampilkan inforasi dokumen 5.selesai
Hasil pengujian	Berhasil

Proses Perhitungan Enkripsi Dengan Algoritma SHA-1

Pada tabel 4.8 merupakan kode program untuk melakukan perhitungan dengan sha-1 pada proses enkripsi, yang selanjutnya akan dibuat *flow graph* dari kode program tersebut.

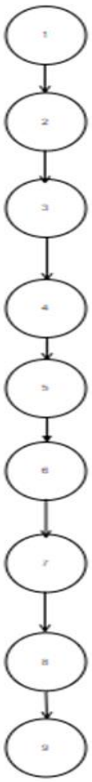
```
var blockstart;                                                    1
        var i, j;
        var W = new Array(80);
        var H0 = 0x67452301;
        var H1 = 0xEFCDAB89;
        var H2 = 0x98BADCFE;
        var H3 = 0x10325476;
        var H4 = 0xC3D2E1F0;
        var A, B, C, D, E;
        var temp;
        msg = Utf8Encode(msg);
        var msg_len = msg.length;
        var word_array = new Array();
        for (i = 0; i < msg_len - 3; i += 4) {                     2
j = msg.charCodeAt(i) << 24 | msg.charCodeAt(i + 1)
 << 16 | msg.charCodeAt(i + 2) << 8 |
msg.charCodeAt(i + 3);
word_array.push(j);
        }
        switch (msg_len % 4) {
                case 0:
                        i = 0x080000000;
                        break;                                     3
                case 1:
        i = msg.charCodeAt(msg_len - 1) << 24 |
0x0800000;
```

```
                    break;
                case 2:
i = msg.charCodeAt(msg_len - 2) << 24 | msg.charCodeAt(msg_len - 1)
 << 16 | 0x08000;
                    break;
                case 3:
i = msg.charCodeAt(msg_len - 3) << 24 | msg.charCodeAt(msg_len - 2)
<< 16 | msg.charCodeAt(msg_len - 1) << 8 | 0x80;
                    break;
            }
            word_array.push(i);
            while ((word_array.length % 16) != 14) word_array.push(0);
            word_array.push(msg_len >>> 29);
            word_array.push((msg_len << 3) & 0x0ffffffff);
for (blockstart = 0; blockstart < word_array.length; blockstart += 16) {
            for (i = 0; i < 16; i++) W[i] = word_array[blockstart + i];
for (i = 16; i <= 79; i++) W[i] = rotate_left(W[i - 3] ^ W[i - 8] ^ W[i - 14]
 ^ W[i - 16], 1);
                A = H0;
                B = H1;
                C = H2;
                D = H3;
                E = H4;
                for (i = 0; i <= 19; i++) {
temp = (rotate_left(A, 5) + ((B & C) | (~B & D)) + E + W
[i] + 0x5A827999) & 0x0ffffffff;
                    E = D;
                    D = C;
                    C = rotate_left(B, 30);
                    B = A;
                    A = temp;
                }
                for (i = 20; i <= 39; i++) {
temp = (rotate_left(A, 5) + (B ^ C ^ D) + E + W[i] + 0x6ED9EBA1) & 0x0ffffffff;
                    E = D;
                    D = C;
                    C = rotate_left(B, 30);
```

```
                    B = A;
                    A = temp;                                   9
                }
                for (i = 40; i <= 59; i++) {
temp = (rotate_left(A, 5) + ((B & C) | (B & D) | (C &
D)) + E + W[i]
+ 0x8F1BBCDC) & 0x0fffffff;
                    E = D;
                    D = C;
                    C = rotate_left(B, 30);
                    B = A;
                    A = temp;      }
                for (i = 60; i <= 79; i++) {
temp = (rotate_left(A, 5) + (B ^ C ^ D) + E + W[i] +
0xCA62C1D6)
 & 0x0fffffff;     E = D;
                D = C;
                C = rotate_left(B, 30);
                B = A;
                A = temp;
        } H0 = (H0 + A) & 0x0fffffff;
        H1 = (H1 + B) & 0x0fffffff;
        H2 = (H2 + C) & 0x0fffffff;
        H3 = (H3 + D) & 0x0fffffff;
        H4 = (H4 + E) & 0x0fffffff;
        }var temp = cvt_hex(H0) + cvt_hex (H1)
+cvt_hex(H2) + cvt_hex(H3) + cvt_hex(H4); return
temp.toLowerCase();}
```

Tabel 4.4
Kode Program Proses Perhitungan SHA-1

Pada gambar 4.28 akan menampilkan *flow graph* dari menampilkan perhitungan dengan algoritma sha-



Gambar 4.19 *Flow Graph* Perhitungan Dengan Algoritma Sha-1(Dwi Suprapti, Made Kamisutara, Putu Artaya,2017)

Dapat dihitung kompleksitas *cyclomatic* sebagai berikut:
V(G) = E – N + 2
= 8 – 9 + 2
= 1
Independent path yang terdapat pada *flow graph* enkripsi file pada Gambar 4.28 yaitu:
Jalur 1: 1-2-3-4-5-6-7-8-9
Dari hasil pengujian menunjukkan terdapat 1 *Independent path* dari fungsi file enkripsi . Tabel 4.4 menunjukkan skenario uji dari perhitungan yang sudah dilakukan.
Tabel 4.8 hasil Pengujian Skenario Menampilkan perhitngan enkripsi dengan algoritma sha-1.
Tabel 4.5 Skenario Kode Program Proses Perhitungan SHA-1

Jalur	Skenario Uji	Hasil yang Diharapkan	Hasil yang Didapatkan	Status
1	Melihat dokumen yang telah dienkripsikan dengan algoritma sha-1 oleh sistem	Menampilkan File yang Telah Di enkripsikan	Menampilkan File yang Telah Di enkripsikan	Valid

Analisis Hasil Pengujian

Berdasarkan hasil pengujian White Box pembuatan flowchart, pembuatan flow graph, perhitungan kompleksitas siklomatis, perhitungan jalur independen, dan test case dapat dirincikan sebagai berikut:

1. Proses Login

Hasil perhitungan *siklomatis* dari Login adalah 2, *independent path* 2 dan test case 2. Setiap test case diujikan dan mendapatkan hasil yang valid, dengan tipe prosedur yang sederhana dan tingkat resiko yang rendah.

2. Proses Upload Dokumen

Pada hasil perhitungan *siklomatis* dari Upload Dokumen adalah 2, *independent path* 2 dan test case 2. Setiap test case diujikan dan mendapatkan hasil yang valid dengan tipe prosedur yang sederhana dan tingkat resiko yang rendah.

3. Proses Scan Dokumen

Hasil perhitungan *siklomatis* dari SCAN Dokumen adalah 2, *independent path* 2 dan test case 2. Setiap test case 2 diujikan dan mendapatkan hasil yang valid dengan tipe prosedur yang sederhana dan tingkat resiko yang rendah.

Berdasarkan rincian pengujian *White Box* Testing diatas dapat dinyatakan bahwa *website* telah bekerja sama dengan baik sesai dengan yang semestinya dibuat,dalam hal proses *input* maupun *output*, hal ini didasarkan pada beberapa hasil pengujian seperti pengujian proses login, proses upload dokumen, proses scan dokumen.

4. Proses Perhitungan Enkripsi Dengan Algoritma SHA-1

Pada hasil perhitungan *cyclomatic complexity* dari Menampilkan Enkripsi dari dokumen adalah 1, *independent path* 1 dan Uji kasus 1. Setiap uji kasus diujikan dan mendapatkan hasil yang valid dengan tipe prosedur yang sederhana dan tingkat resiko yang rendah.

Kesimpulan

Berdasarkan tahap implementasi dan pengujian yang telah dilalui maka dapat diambil kesimpulan sebagai berikut:

1. Penerapan digital signature pada sektor Pertanian,ketahanan pangan dan perikanan Kab.Mempawah berhasil dilakukan
2. Penerapan algoritma SHA-1 pada dokumen surat telah berhasil terenkripsi dari data aslinya.
3. Keaslian dokumen elektronik dapat diverifikasi.
4. Digital signature menggunakan SHA-1 merupakan salah satu alternatif dalam pengamanan data sehingga pihak-pihak yang berkaitan terhadap data tersebut dapat merasa yakin bahwa data tersebut aman

Saran

Berikut adalah beberapa saran terkait penelitian selanjutnya yang dapat dilakukan berdasarkan Penelitian yang telah dilakukan, yaitu:

1. Membangun aplikasi berbasis android untuk penerapan digital signature.
2. Menerapkan pada dokumen dengan format berbeda.
3. Akan terus memperbarui karena ilmu pengetahuan selalu berkembang maka untuk selanjutnya dapat dilakukan penelitian terhadap SHA yang lebih baru, atau dapat meneliti algoritma hash selain SHA-1.

DAFTAR PUSTAKA

KOMINFO. (2018). Penggunaan Tanda Tangan Digital di Indonesia Tumbuh Pesat.Kromodimoeljo, S. (2010). Teori Dan Aplikasi Kriptografi. Jakarta.

Bandung: Informatika Bandung. Munir, R. (2006). Kriptografi. Bandung: Informatika Bandung.
Refialy, L. (2015). Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA. Rionaldy, R. (2017).
Implementasi RSA sebagai Digital Signature pada Publikasi Arsip Elektronik Berbasis Web. Republik Indonesia. 1972. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jakarta
Aulia Nadzifarin dan Asmunin. (2022). Penerapan Elliptic Curve Digital Signature Algorithm pada Tanda Tangan Digital dengan Studi Kasus Dokumen Surat – Menyurat.
Agung Purnomo Sidik. (2022). Mendeteksi Keaslian Data Menggunakan Kombinasi Message Digest-5 dengan RSA Public Key Algorithm. Jurnal Sains dan Informatika.
Vicky Hernando Zulian dan Purwanto Purwanto.(2022). Implementasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma ELGAMAL Pada Dokumen Di Balai Pendidikan Dan Pelatihan Penerbangan (BP3) Curug Berbasis Web.
Rezky M. Nasution.(2022). Implementasi Metode Secure Hash Algorithm (SHA-1) Untuk Mendeteksi Orisinalitas File Audio. https://hostjournals.com.
Diki Arisandi,Sukri dan Moh.Baharudin Yusuf.(2020). Pemeriksaan Integritas Dokumen Dengan Digital Signature Algorithm. JOISIE Journal Of Information System And Informatics Engineering.
Ariyus, D., Kriptografi Keamanan Data dan Komunikasi, Graha Ilmu, Yogyakarta, 2008
Refialy, L. (2015). *Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA*.
Kromodimoeljo, S. (2010). *Teori Dan Aplikasi Kriptografi*. Jakarta.

Abdulloh, Rohi. (2016). Easy dan Simple Web Programming. Jakarta: Elex Media. Komputindo

Enterprise J. 2015. Mengenal PHP Menggunakan Framework Laravel. PT. Elexmedia Komputindo Jakarta.