IMPLEMENTASI DIGITAL SIGNATURE PADA ARSIP DI DINAS KEARSIPAN PROVINSI SUMATERA SELATAN

Arpa Pauziah[1], M.Izman Herdiansyah[2]
Program Studi Magister Tehnik Informatika, Universitas Bina Darma, Palembang[1,2]
E-mail: arpa.pauziah@gmail.com[1],m.herdiansyah@binadarma.ac.id[2]

Abstrak

Saat ini *digital signature* atau bisa juga disebut dengan tanda tangan digital sudah semakin banyak digunakan terutama terhadap suatu arsip. Teknologi arsip digital dianggap sebagai berbeda dari arsip tradisional yang mengacu pada kelestarian objek fisik seperti Photo, Filmdan Kartografi yang dapat membawa informasi. Pentingnya tingkat keamanan yang tepat dalam menjaga keaslian arsip tersebut maka diperlukan tanda bukti yang kuat yaitu berupa *digital signature* (tanda tangan digital) yang dapat di akses melalui Smartphone Android,kemudian dokumen tersebut akan diberikan *digital signature* berupa *hybrid Cryptosystem*yang digunakan untuk enkripsi dan deskripsi pesan dengan memakai algoritma RSA (*Rivest Shamir Adleman*) dan algoritma AES (*Advanced Encryption Standard*). Adapun alasan menggunakan teknik *Hybrid Cryptosystem* supaya lebih aman dan efisien.

Kata kunci: *Digital Signature, Hybride Cryptosystem,RSA,AES*

Abstract

Currently digital signatures or can also be called digital signatures are increasingly being used, especially for an archive. Digital archival technology is considered as different from traditional archives which refers to the preservation of physical objects such as Photo, Film and Cartography that can carry information. The importance of the right level of security in maintaining the authenticity of the archive requires strong evidence in the form of a digital signature that can be accessed via an Android Smartphone, then the document will be given a digital signature in the form of a hybrid Cryptosystem used for encryption and message description. using the RSA (Rivest Shamir Adleman) algorithm and the AES (Advanced Encryption Standard) algorithm. The reason for using the Hybrid Cryptosystem technique is to make it more secure and efficient.

Keywords: *Digital Signature, Hybride Cryptosystem,RSA,AES*

I PENDAHULUAN

Saat ini *digital signature* atau bisa juga disebut dengan tanda tangan digital sudah semakin banyak digunakan terutama terhadap suatu arsip. Hal tersebut karena tanda tangan digital bisa dikatakan dapat menjamin arsip tersebutapakah memang benar hasil karya pemiliknya atau mungkin telah dimodifikasi oleh pihak lain dalam hal penyampaiannya. Teknologi arsip digital dianggap sebagai berbeda dari arsip tradisional yang mengacu pada kelestarian objek fisik seperti Photo, Filmdan Kartografi yang dapat membawa informasi. Dengan kata lain dapat dijelaskan bahwa arsip seringkali merupakan tempat dalam organisasi yang diperlukan untuk menyimpan dan mengatur catatan organisasi yang memiliki nilai tinggi dan bertahan lama.

Proses pengelolaan arsip digital pada Dinas Kearsipan Provinsi Sumatera Selatan sudah mulai dilakukan dengan cara arsip yang berupa lembaran kertas di scan lalu disimpan didalam folder, begitu pula dengan file yang berupa gambar, video, dan rekaman suara semuanya dimasukan di dalam folder yang berbeda-beda sesuai dengan jenis arsip tersebut. Namun tentu saja dalam segi keamanan cara seperti ini kurang tepat karena arsip tersebut bisa saja di ambil alih oleh orang lain dan disalah gunakan.

Mengingat pentingnya tingkat keamanan yang tepat dalam menjaga keaslian arsip tersebut maka diperlukan tanda bukti yang kuat yaitu berupa *digital signature* (tanda tangan digital) yang dapat di akses melalui Smartphone Android, dimana arsip atau dokumen cetak akan di Scan dalam bentuk file PDF, kemudian dokumen tersebut akan diberikan *digital signature* berupa *hybrid Cryptosystem*yang digunakan untuk enkripsi dan deskripsi pesan dengan memakai algoritma RSA (*Rivest Shamir Adleman*) dan algoritma AES (*Advanced Encryption Standard*). Selanjutnya dokumen yang telah diberi *digital signature*, akan disajikan di Daftar arsip. Dimana di daftar arsip tersebut semua orang bisa melihat dan mencari daftar arsip yang ada, namun mereka tidak bisa melihat isi dari file tersebut. Untuk bisa melihat isi file tersebut harus menghubungi orang yang memegang kunci private, adapun kunci private yang akan digunakan untuk mendeskripsikan file yaitu berupa RFID Tag (*Radio Frequency Identification*) yang disisipkan kedalam sebuah kartu. Kartu tersebut dapat dibaca oleh smartphone android yang memiliki fiture NFC (*Near Field Communication)*. Adapun alasan menggunakan teknik *Hybrid Cryptosystem* supaya lebih aman dan efisien.

Berdasarkan uraian diatas, maka penulis tertarik untuk mengangkat judul tesis yaitu **"Implementasi Digital Signature pada Arsip di Dinas Kearsipan Provinsi Sumatera Selatan".**

II TINJAUAN PUSTAKA

2.1 Tanda Tangan Digital

Tanda tangan digital merupakan tanda tangan yang dilakukan dengan memakai alat elektronik yang berfungsi sama dengan tanda tangan manual. Tanda tangan digital merupakan kumpulan bit yang bisa melakukan fungsi elektronik yang memakai fungsi Hash satu arah [5].

Tujuan tanda tangan dalam dokumen adalah untuk memastikan keaslian dokumen. Transaksi elektronik juga menggunakan tanda tangan digital atau dikenal sebagai *Digital Signature. Digital Signature* sebenarnya bukan tanda tangan karena telah dikenal sejak lama, yang menggunakan metode berbeda untuk menandai dokumen sehingga dokumen atau data tidak hanya mengidentifikasi pengirim, tetapi juga memastikan bahwa integritas dokumen tidak berubah selama proses transmisi. Tanda tangan digital didasarkan

pada konten pesan itu sendiri. Sejauh ini, tanda tangan digital adalah metode keamanan dalam penggunaan jaringan publik sebagai sarana transfer data yang cukup aman. Dikatakan aman karena tanda tangan digital terbentuk dari serangkaian algoritma yang sangat sulit bukan berarti tidak bisa. Beberapa bentuk kejahatan dalam pemalsuan tanda tangan digital menggunakan perangkat lunak yang dapat menghasilkan tanda tangan digital [3].

Sifat yang dimiliki oleh d*igital signature* atau tanda tangan digital adalah :

1. Autentik, tidak bisa / sukar ditulis / jiplak oleh orang lain. Kata-kata dan tanda tangan pesannya itu juga bisa menjadi barang bukti sehingga penanda tangan tidak bisa mengakui bahwa dahulunya ia pernah menandatangani arsip tersebut.
2. Hanya sah atau dapat diterima oleh dokumen (pesan) itu saja atau versi copy yang sama persis. Tanda tangan tersebut tidak bisa dipindahkan ke dokumen lain walaupun dokumen lain itu cuma berbeda sedikit. Dan juga jika dokumen tersebut diubah oleh orang lain maka *digital signature* atautanda tangan digital dari pesan tersebut tidak lagi dikatakan sah.
3. Bisa diperiksa dengan mudah, termasuk oleh orang yang belum pernah bertemu atau bertatap muka langsung dengan penandatangan tersebut [4].

Dalam pemberian tanda tangan terhadap suatu dokumen digital, dapat menggunakan dua alternatif yaitu :

1. Gunakan enkripsi pesan
2. Gunakan fungsi hash dan kriptografi kunci publik

Untuk altenatif penggunaan enkripsi pesan sendiri, memiliki dua alternatif juga yaitu denganmemakai kunci simetri atau kunci publik.

Jika telah menggunakan alternatif enkripsi pesan dan kunci simetri maka metode ini sudah memberikan solusi yang tepat untuk otentikasi pengirim dan keaslian pesan, karena kunci tersebut hanya diketahui oleh pengirim dan penerima pesan [9].

2.2 Kriptografi

Menurut Meneze dkk (2014) yang dikutip oleh (Jamaludin 2020:7), menyatakan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data dan otentikasi. Jadi dapat disimpulkan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamanan informasi. Cara melakukan teknik ini mulanya pengirim pesan akan melakukan penyandian pesan awal yang menjadi kode-kode yang hanya dapat dibaca oleh penerima tersebut. Selanjutnya, penerima pesan mengembalikan kode-kode yang telah diterima menjadi pesan asli dengan menggunakan kunci yang dikirimkan oleh pengirim pesan. [10].

Kriptografi sering diminta untuk melakukan pekerjaan sebagai berikut :

1. Kerahasiaan (*confidentiality*) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan. Didalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi pesan yang tidak bisa terbaca oleh pihak yang berhak.
2. Autentikasi (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication)* maupun mengidentifikasi kebenaran dari sumber pesan (*data origin authentication)*. Dua pihak yang saling

berkomunikasi harus dapat mengidentifikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diautentikasi sumbernya.

3. *Data integrity*atauintegritas data merupakan layanan yang dapatr menjamin bahwa pesan tersebut masih asli dan belum pernah dilakukan manipulasi selama dalam proses pengiriman. Untuk menjaga keutuhan data, system harus mempunyai kemampuan dalam mendeteksi rekayasa pesan yang dilakukan oleh pihak yang tidak berhak, antara lain perubahan, menghapus dan penyisipan data lainnya kedalam pesan yang sebenarnya. Didalam kriptografi layanan ini direlisasikan dengan menggunakan tanda tangan digital (*digital signature).*
4. Tidak ada penyangkalan (*non-repudiation)* adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. [11]

2.3 Hash

Menurut (Nurhasanah, Tanpa tahun : 1), Dalam ilmu kriftografi terdapat suatu fungsi yang dapat dipakai untuk sebuah aplikasi keamanan seperti menjaga otentikasi dan integritas pesan. Fungsi yang dimaksud adalah fungsi hash. Fungsi hash yaitu fungsi yang digunakan untuk menerima barisan dengan panjang sebarang dan mengubah bentuk teks menjadi barisan hingga hasil keluaran yang panjangnya tertentu. Fungsi hash dapat menerima masukan barisan hingga apasaja. Jika barisan hingga menyatakan pesan M, maka sebarang pesan M berukuran bebas dimanfaatkan oleh fungsi hash H melalui persamaan : h = H (M).[6]

Fungsi Hash merupakan fungsi yang menerima masukan string yang panjangnya sembarang serta mengonversinya menjadi teks atau string keluaran yang panjangnya tetap (*fixed),* pada umumnya berukuran jauh lebih kecil daripada ukuran yang semula [5].

Fungsi Hash satu arah atau *one-way hash function yang* berfungsi sebagai :

1. Sidik jari (*fingerprint) :*Membuat sidik jari dari suatu dokumen atau pesan M yang mana sidik jari merupakan suatu identitas dari si pengirim pesan.
2. Fungsi kompresi : Fungsi kompresi, dokumen D yang besarnya masukan lebih besar dari pada keluaran, seolah-olah mengalami kompresi, namun hasil dari kompresi tidak bisa dikembalikan ke bentuk awalnya, yang oleh karenanya dinamakan satu arah.
3. Messages digest : Dianggap intisari dari suatu dokumen, padhal tidak demikian karena dengan sidik jari orang lain tidak mengerti asli dari dokumen tersebut.

2.4 Algoritma RSA

Menurut (Respationo, Tanpa tahun: 2), Algoritma RSA diambil dari nama ketiga orang pengembangnya yaitu Ron (R)ivest, Adi (S)hamir, Leonard (A)dleman. Algoritma ini memiliki kekuatan berupa sulitnya mencari faktor prima dari bilangan yang besar. Secara garis besar algoritma ini cukup sederhana, hanya terdiri dari fungsi pangkat dan modulo saja [7].

Algoritma yang paling popular yaitu algoritma RSA. Karena banyak pengguna yang menggunakan algoritma untuk keperluan kriptografi kunci-publik, Algoritma ini memfaktorkan bilangan yang sangat besar. Oleh sebab itu RSA bisa dikatakan aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang

besar. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute Of Technology) pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. RSA mengekspresikan teks-asli yang di enkripsi menjadi blok-blok yang mana setiap blok memiliki bilangan biner yang diberi symbol "n", blok teks asli "M" dan blok teks-kode "C". untuk melakukan enkripsi pesan "M", pesan dibagi kedalam blok-blok numerik yang lebih kecil daripada "n" (data biner dengan pangkat besar). Jika bilangan prima yang panjangnya 200 digit, dapat ditambah beberapa bit 0 dikiri bilangan untuk menjaga agar pesan tetap kurang dari nilai "n" [5].

2.5 Tanda Tangan Digital Menggunakan Algoritma RSA

Berikut algritma secara singkat [11]:

1. Pilih 2 bilangan prima *p* dan *q* yang cukup besar.
2. Hitung $n=p*q$ dan hitung $\phi(n)=(p-1)*(q-1)$.
3. Pilih kunci publik *e* yang relatif prima terhadap $\phi(n)$.
4. Bangkitkan kunci private dengan ketentuan $e*d \equiv 1 (mod \phi(n))$
5. Enkripsi dengan cara membagi plainteks menjadi blok-blok sehingga setiap blok mempresentasikan nilai dalam selang [0..n-1]
6. Tiap lok akan dikenakan fungsi $c_i \equiv p_i^e (mod\ n)$.
7. Deskripsi dilakukan dengan fungsi yang sama terhadap setiap blok hanya dengan kunci yang berbeda. $p_i \equiv c_i^d (mod\ n)$.

Pada pemberian tanda tangan digital, enkripsi dilakukan dengan kunci privat. Dan saat verivikasi tanda tangan dilakukan deskripsi dengan kunci publik.

2.6 Algoritma AES (*Advance Encription standard)*

AES merupakan system penyandian blok yang bersifat non- Feistel karena AES menggunkan komponen yang selalu memiliki invers dengn panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Pross didalam AES merupakan transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state secara berulang dalam beberapa ronde. State yang menjadi keluarga ronde k menjadi masukan untuk ronde ke-k+1. [16]

2.7 *Hybride Cryptosystem*

Hybride Cryptograph merupakan teknik kriptografi dengan menggunakan dua atau lebih *cipher* yang berbeda dalam waku bersamaan. Sedangkan *HybrideCryptosystem* untuk melakukan enkripsi atau deskripsi pesan yang panjang akan efisien dengan menggunakan *symetryc-key*. Sedangkan kunci publik hanya digunakan untuk mengenkripsi / mendeskripsi kunci simetris yang pendek [15].

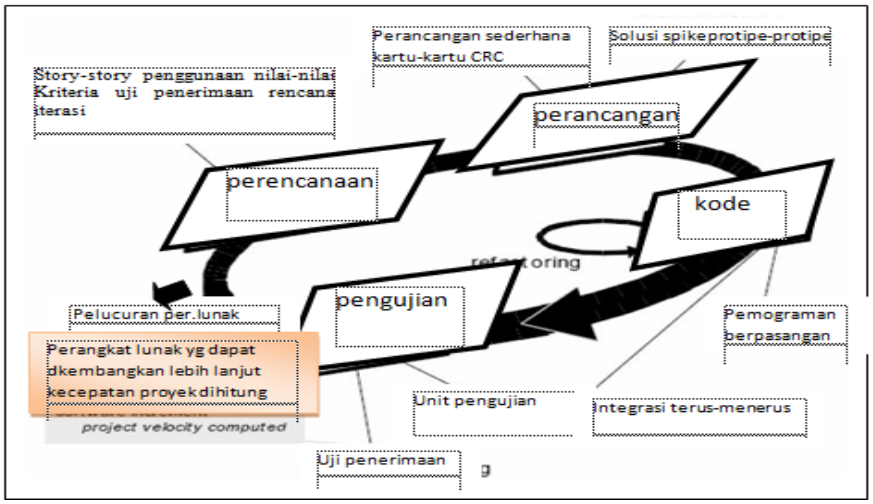
III METODOLOGI PENELITIAN

3.1 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah menggunakan metode *Extreme Programming.* XP*(Extreme* Programming) merupakan salah satu metodologi rekayasa perangkat lunak yang banyak digunakan untuk mengembangkan aplikasi oleh para developer. XP sangat cocokuntuk pengembangan proyek yang memerlukan adaptasi cepat dalam perubahan-perubahan yang terjadi selama pengembangan aplikasi. XP juga cocok untuk anggota tim yang tidak terlalu banyak dan berada pada lokasi

yang sama dalam pengembangan system [1].

Berikut adalah gambar model *Extreme Programing* dapat dilihat pada gambar:



Gambar 1. Metode Extreme Programing

Adapun tahapan dari metode Extreme Programing yang terdapat pada Gambar 1 terdiri dari beberapa tahapan yaitu :

1. Perencanaan

   Pada tahap perencanaan ini dimulai dari pengumpulan kebutuhan yang membantu tim teknikal untuk memahami konteks bisnis dari sebuah aplikasi. Selain itu pada tahap ini juga mendefinisikan output yang akan dihasilkan, fitur yang dimiliki oleh aplikasi dan fungsi dari aplikasi yang dikembangkan.

2. Desain

   Metode ini menekankan desain aplikasi yang sederhana, untuk mendesain aplikasi dapat menggunakan *Class-Responsipility-Collaborator* (CRC) cards yang mengidentifikasi dan mengatur class pada object-oriented.

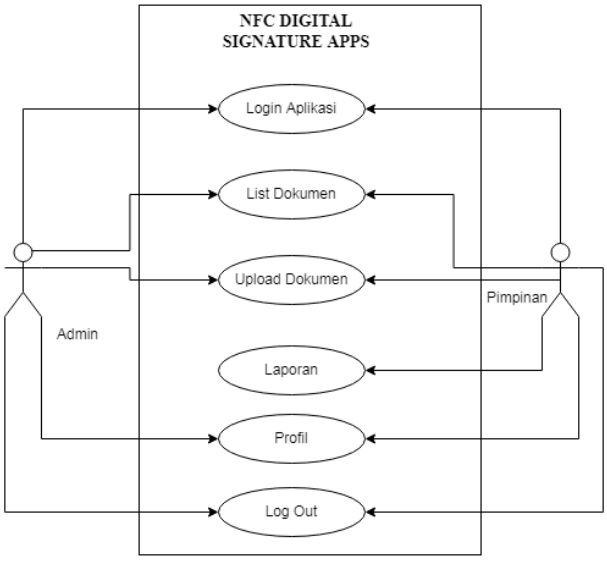
3. Pengkodean

   Konsep utama dari tahapan pengkodean pada extreme programing adalah pair programing, melibatkan lebih dari satu orang untuk menyusun kode.

4. Pengujian

   Pada tahapan ini lebih fokus pada pengujian fitur dan fungsionalitas dari aplikasi.

3.2 Use Case Diagram



Gambar 2. Use Case Diagram

Berdasarkan gambar 2 *Use Case Diagram* Aplikasi Digital Signature pada Arsip, dapat diuraikan sebagai berikut :

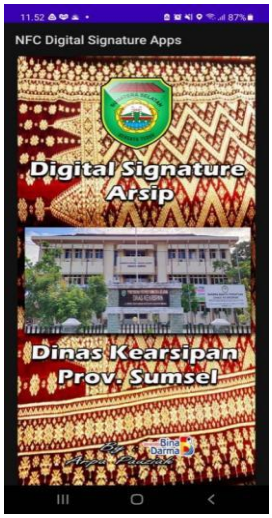
1. Admin : Peran admin pada aplikasi ini yang memegang kartu RFID Tag dan yang akan bertanggung jawab pada Aplikasi Digital Signature Arsip.
2. Pimpinan : Bisa memantau aplikas, terutama laporan data arsip yang tidak bisa dilihat oleh admin.
3. Login : Sebelum masuk ke menu utama, Admin dan Pimpinan harus melakukan login terlebih dahulu.
4. Pada menu list document, Admin dan Pimpinan dapat melihat daftar dokumen arsip. Namun ketika untuk membuka dan penghapusnya, Admin memerlukan dua kunci, yang pertama kunci password yang dimasukan saat upload dokumen. Kunci kedua yaitu NFC tag, yang berupa kartu ID.
5. Selanjutnya pada menu upload dokumen, Admin mengklik tombol pilih file untuk memipih file dengan format PDF yang telah di siapkan untuk di upload. Kemudian isikan judul file pada kolom judul, masukan deskripsi atau sedikit penjelasan tentang file tersebut. lalu masukan juga kunci dokumen dapat berupa angka atau huruf, kunci dokumen ini jangan sampai lupa karena akan diperlukan untuk membuka file. Langkah terakhir dengan mengklik tombol ambil kunci NFC, lalu tempelkan kartu ID tepat di belakang smartphone agar dapat mendeteksi RFID. Jangan lupa menekan tombol simpan dokumen.
6. Laporan hanya dapat dilihat oleh Pimpinan.
7. Pada menu logout, berfungsi untuk mengakhiri dan user akan keluar dari akun tersebut.

IV HASIL DAN PEMBAHASAN

4.1 Tampilan Aplikasi

1. Tampilan *Splash Screen*

Berikut adalah tampilan *splash screen* atau tampilan pembuka, digunakan untuk menampilkan halaman awal, dapat dilihat pada gambar 3 :



Gambar 3. Hasil Tampilan Hamanan *Splash Screen*

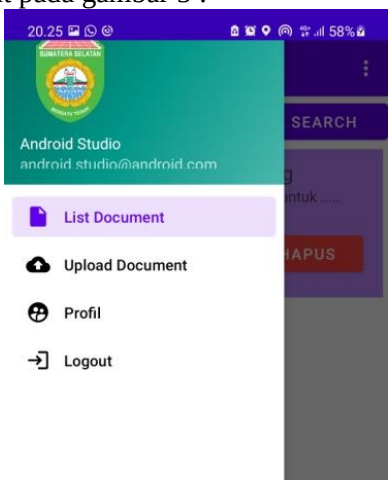
2. Tampilan Halaman Login

Sebelum masuk ke menu utama, admin harus melakukan login terlebih dahulu. Halaman login yang digunakan untuk masuk kedalam Aplikasi *Digital Signature* arsip admin atau pimpinan login dengan menginput email dan password kemudian menekan tombol login. Apabila belum memiliki akun dapat menekan tombol daftar dan melakukan registrasi Berikut adalah tampilan halaman login dapat dilihat pada gambar 4 :

Gambar 4. Hasil Tampilan Halaman Login

3. Tampilan Halaman Menu Utama

Pada menu utama terdapat list document untuk melihat daftar-daftar arsip, upload document untuk menambahkan daftar arsip, profile untuk melihat profile dan yang terakhir yaitu menu logout yang digunakan untuk keluar dari aplikasi. Tampilan halaman menu utama dapat dilihat pada gambar 5 :



Gambar 5. Tampilan Halaman Menu Utama

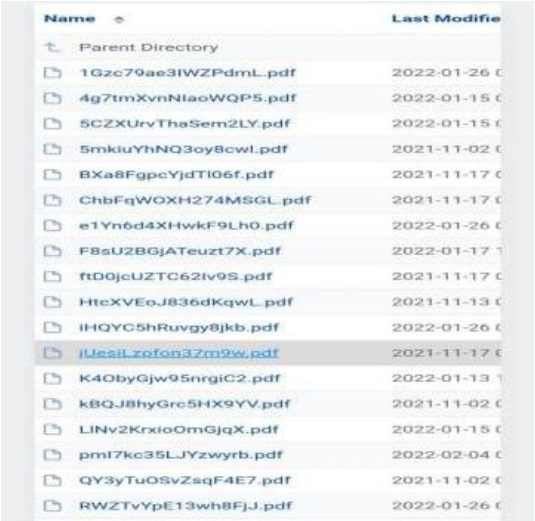
4. Tampilan Halaman List Document

Tampilan list document terdapat daftar-daftar arsip dan memiliki 3 tombol yaitu search berfungsi untuk mencari data, tombol buka mengarahkan ke tampilan buka dokumen dan tombol hapus mengarah pada tampilan hapus file. Tampilan halaman list document dapat dilihat pada gambar 6 :

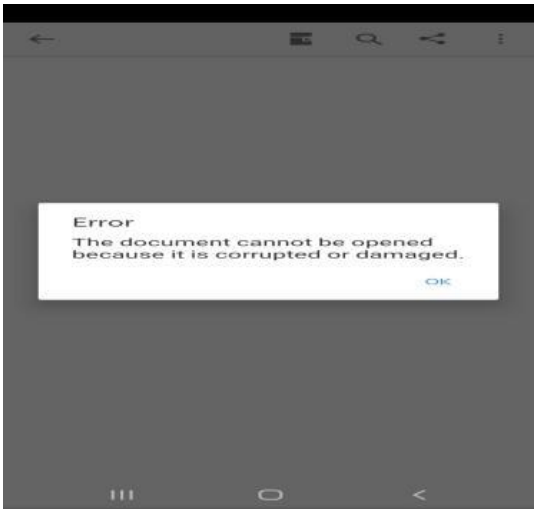
Gambar 6. Tampilan Halaman List Document

5. Tampilan Hasil Status Enkripsi Pada Aplikasi Digital Signature Arsip

Hasil status enkripsi pada dokumen yang telah diberikan tandatangan digital bisa dilihat pada gambar 7 yang merupakan gambar dari daftar arsip yang tersimpan di dalam server. File yang ada pada gambar 7 tersebut jika di klik maka tampilannya akan seperti pada gambar 8 yang berarti bahwa gambar tersebut tidak dapat dibuka. Untuk bisa membuka file yang di pilih, maka diperlukan aplikasi digital signature arsip. Berikut ini gambar 8 dan gambar 8 :



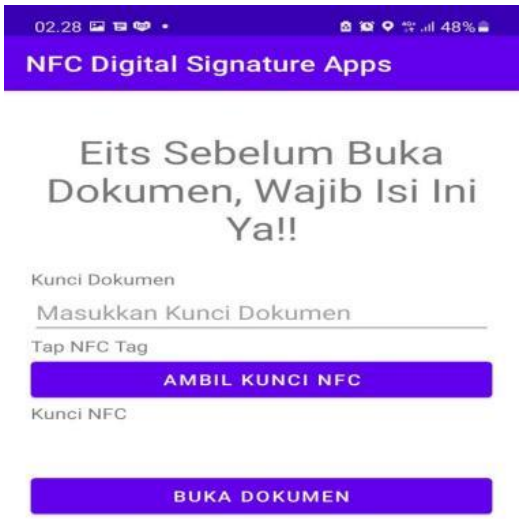
Gambar 7. Tampilan Daftar Arsip Yang tersimpan Di Server



Gambar 8. Tampilan PDF Yang Tidak Bisa Dibuka Karena Telah Diamakan Oleh Digital Signature

6. Tampilan Halaman Buka Document

Pada halaman buka document, akan diminta untuk menempelkan kartu RFID jika kunci dokumen berhasil dimasukan dan NFC tag berhasil mendeteksi maka dokumen dapat di buka. Tampilan halaman buka document dapat dilihat pada gambar 9 :



Gambar 9. Tampilan Halaman Buka Document

7. Tampilan Halaman Upload Document

Halaman upload dokumen akan tampil ketika admin menekan upload document yang ada pada menu utama. Tombol pilih file akan mengarahkan ke tempat penyimpanan file, kemudian admin diminta untuk mengisi judul arsip, deskripsi dari isi arsip tersebut, mengisi kunci dokumen yang harus di ingat ketika akan membuka file, dan yang terakhir menekan tombol ambil kunci NFC lalu admin menempelkan kartu RFID, setelah kartu RFID terbaca, admin adapat menyimpan dokumen. Tampilan halaman upload document dapat dilihat pada gambar 10 :

Gambar 10. Tampilan Halaman Upload Document

8. Tampilan Halaman laporan

Halaman laporan hanya dapat dilihat oleh pimpinan. Pimpinan dapat menekan tombol tanggal mulai untuk menampilkan kalender dan pimpinan memilih tanggal mulai laporan yang di inginkan untuk menentukan batas mulai laporan yang akan ditampilkan, begitupun tombol tanggal selesai guna untuk menentukan batas akhir laporan yang di inginkan. Berikut ini tampilan halaman ubah laporan dapat dilihat pada gambar 11:

Gambar 11. Tampilan Halaman Laporan

9. Tampilan Kartu RFID Tag

Letak Digital Signature terletak pada RFID Tag ini, kartu ini yang akan digunakan pada saat membuka, menghapus maupun menambahkan dokumen. Tampilan Kartu RFID Tag, dapat dilihat pada gambar 12 :

Gambar 12. Tampilan Kartu RFID Tag

4.2 Hasil Pengujian

Dalam pengujian kali ini penulis menggunakan 20 sampel file arsip statis yang telah disimpan dalam format pdf. Pada file tersebut akan diuji kecepatan waktu per mili second serta ukuran file size per kilobyte.

Berikut ini tabel dari hasil pengujian enkripsi dan deskripsi pada aplikasi digital signature pada arsip:

Tabel 1 Hasil Pengujian

NO	Nama File	Ukuran File Sebelum di Enkripsi (Kilo Byte)	Ukuran File Setelah di Enkripsi (Kilo Byte)	Waktu Enkripsi (Mili Second)	Waktu Deskripsi (Mili Second)
1	Surat kontrak perdagangan antara Sultan Ratu Abdul Jamal dengan Gubernur Jendral Rijkloft	83	164	798	171
2	Daftar nama peserta rapat tanjung jati	98	195	656	230
3	Denah Pemerintahan Kota Palembang Tahun 1819	49	96	344	118
4	Keputusan Presiden RI Nomor 107 tahun 1953 tentang Pedoman Bekerja untuk Dewan Pemerintah Daerah Sementara Provinsi Sumatera Selatan tanggal 16 Juni 1953	59	116	368	126
5	Keputusan Presiden Republik Indonesia Serikat (RIS) Nomor 120 tahun 1950 tentang Pengangkatan Dr. M.Isa sebagai Komisaris Pemerintah RIS untuk Negara Sumatera Selatan tanggal 17 Maret 1950	55	109	361	118
6	Keputusan Presiden RI Nomor 96 tahun 1963 tentang Pengangkatan Kiagus Syafaruddin sebagai Anggota MPRS Wakil dari Daerah Sumatera Selatan tanggal 14 Mei 1963	55	109	353	120
7	Keputusan Presiden Republik Indonesia Serikat (RIS) Nomor 155 Tahun 1950 tentang Pembahasan Tugas Dr. Mohammad Isa sebagai Komisaris Pemerintah RIS Negara Sumatera Selatan tanggal 19 April 1950	37	73	251	85
8	Peta Palembang dengan Sungai Musi Talang Betutu Tahun 1945	63	124	404	131

9	Peta Sekayu, Muara Enim, Perbatasan Riau, Jambi dan Bangka tahun 1941	48	94	527	105
10	Peta Residensi Palembang Tahun 1922	49	96	394	106
11	Keputusan Presiden RI Nomor 63 Tahun 1951 tentang pengangkatan Dr. Mohammad Isa sebagai Gubernur / Kepala Daerah Otonom Sematera Selatan tanggal 25 April 1951	57	113	410	125
12	Sketsa Bengkulu dan Palembang tahun 1930	41	81	284	92
13	Sketsa Perbatasan Palembang Rejang dan Ampat Lawang Bengkulu yang merupakan lampiran dari Resolusi Nomor 8 tanggal 29 Juli 1832	58	114	375	124
14	Naskah Sumpah Pelantikan Pangeran Krama Jaja, Perdana Menteri dari Palembang tanggal 5 September 1823	63	125	415	136
15	Surat dari Komisi Resolusi 15 Januari 1830 kepada Gubernur Jendral hindia Belanda tentang Penggabungan Bengkulu dengan Palembang tanggal 15 Maret 1830	66	130	692	145
16	Surat dari Menteri Kesehatan kepada Presiden RI tentang Pendirian Rumah Sakit di Palembang Sumatera Selatan tanggal 23 Juni 1951	75	149	572	152
17	Surat dari Raja Palembang Sultan Ahmad Najamuddin kepada Gubernur Jendral Vander Capellen mengenai keadaan dan kedudukan keluarganya, tanggal 26 November 1823 (22 Rabiul Awal 1239 H)	85	169	816	184
18	Surat Sultan Mohamad Badaruddin dari Palembang kepada Gubernur Jendral Hindia Belanda mengenai keadaannya yang diasingkan ke Ternate tanggal 23 Desember 1823 (12 Safar 1239 H)	75	149	551	158
19	Sketsa Tempat Tinggal / Perkampungan Susuhunan Ratu Mahmud Badaruddin (SMB II) Selama Dalam Pengasingan Di Ternate Maluku Utara	2391	4780	16283	4879
20	Foto Lambang Kota Palembang Tahun 1928	1294	2586	8519	2659

V KESIMPULAN

Kesimpulan yang didapat dari hasil pengerjaan tesis ini berdasarkan hasil proses pengimplmentasian aplikasi yaitu, dengan Aplikasi Digital Signature Pada Arsip dapat memberikan keamanan yang lebih dibandingkan hanya di scan dan di masukan kedalam folder seperti yang telah dilakukan pada Dinas Kearsipan Prov. Sumsel sebelumnya. Apalagi dengan menggunakan kartu RFID Tag, sehingga jauh lebih terjamin keamanan nya.

Aplikasi ini berjalan pada smartphone yang memiliki picture NFC dan minimal android yang digunakan versi 5.1.1 *lollipop.*

VI SARAN

Aplikasi digital signature ini tentu saja masih banyak kekurangannya sehingga saranyang penulis rekomendasikan yaitu dikemudian hari dapat dikembangkan lagi dengan tampilan yang lebih menarik, memberikan penambahan menu.

VII DAFTAR PUSTAKA

[1] Suryantara, 2017. **Merancang Aplikasi dengan Metodologi Extreme Programmings.** Jakarta : Penerbit PT. Elex Media Komputindo

[2] Yo Ceng Giap, dkk. 2020. **Cloud Computing : Teori dan Implementasi.** PenerbitYayasan Kita Menulis.

[3] Nofriansyah, dkk. 2020. **Bisnis Online : Strategi dan Peluang Usaha.** Penerbit Yayasan Kita Menulis.

[4] Stiawan, Deris. 2005. **Sistem Keamanan computer.** Jakarta : Penerbit PT. Elek Media Komputindo.

[5] Ariyus, Dony. 2008. **Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi**. Yogyakarta : Penerbit ANDI

[6] Nurhasanah, Sulaiman. **Pembuatan Tanda Tangan Digital Menggunakan Digital Signatura Algorithm.**Surabaya : Jurusan Matematika, MIPA, Universitas Negeri Surabaya.

[7] Respationo, Unggul Satrio. **Modifikasi Pemberian Digital Signature pada Arsip Citra Menggunakan Gray Code.**Bandung : Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.

[8] Rizaldy, mohamad Ray.**Perbandingan Tanda Tangan Digital RSA dan DSA Serta Implementasinya untuk Antisipasi Pembajakan Perangkat Lunak**.Bandung : Program Studi Teknik Informatika, Institut Teknologi Bandung.

[9] Adipradana, Brahmasta. **Penerapan Tanda Tangan Digital Pada Arsip Stream.**Bandung : Program Studi Teknik Informatika, Institut Teknologi Bandung.

[10] Jamaludin.2020. **Kriptografi : Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA**. Penerbit Yayasan Kita Menulis.

[11] Sari Ika yusnita, dkk. 2020. **Keamanan Data dan Informasi.** Penerbit Yayasan Kita Menulis.

[12] Sarwono,Jonathan. 2010. **Pintar Menulis Karangan Ilmiah.** Yogyakarta: Penerbit ANDI.

[13] Shalahuddin, M, dkk.2013.**Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek**.Bandung : Informatika.

[14] Nazir. 2014. **Metode Penelitian**. Jakarta : Ghalia Indonesia.

[15] Pudoli, Ahmad, Kusmaningsih Dewi. 2017.**Penggunaan Hybrid Cryptosystem untuk Enkripsi dan Deskripsi Pesan Messanger Menggunakan Algoritma Rivest Shamir Adleman (RSA) dan Advanced Encryption Standard (AES) Dengan Firebase Pada Android.** Jakarta Selatan : Fakultas Teknologi Informasi, Universitas Budi Luhur.

[16] Tulloh Aditia Rahmat, dkk. 2016. Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. Bandung : Program Studi Matematika, Universitas Islam Bandung.