

Implementasi Algoritma SHA512 Pada Keamanan Berita Acara Hasil Sidang Berbasis Web

Muhammad Irvai¹, Nolan Efranda²

^{1,2} Informatics Departement, Bina Insan University, Lubuklinggau, Indonesia
Email: ¹muhammadirvai@univbinainsan.ac.id, ²nolanefranda@univbinainsan.ac.id

Abstrak

Masalah pada penelitian ini adalah arsip data berita hasil sidang yang masih disimpan menggunakan *box file* atau masih manual, penyimpanan dan pemeliharaan arsip yang kurang baik, tempat penyimpanan arsip yang tidak terawat dan sulit untuk pencarian arsip sehingga mudah terjadinya kebocoran data. Arsip data yang sangat rahasia agar data terjamin keamanan dan kebocoran data maka dapat dilakukan berbagai cara salah satunya membuat aplikasi yang diintegrasikan dengan kriptografi. Sistem ini dibuat dengan menggunakan Bahasa pemrograman PHP, MySQL digunakan untuk pengelolaan *database* dan implementasi algoritma kriptografi SHA512. Model alur hidup yang digunakan adalah metode *extreme programming*. Dengan adanya penyimpanan berita acara hasil sidang berbasis *website*, kesalahan yang terjadi selama ini dapat diminimalisir. Tujuan aplikasi ini untuk membuat suatu sistem informasi yang mengolah data berita acara hasil sidang sehingga lebih mudah, efektif dan terjamin keamanannya.

Kata Kunci: Algoritma SHA-512, Web, Kriptografi, Berita Acara

1. PENDAHULUAN

Perkembangan teknologi komputer saat ini telah membawa pengaruh dan kemajuan yang pesat dalam berbagai bidang termasuk instansi pemerintahan. Hal ini disebabkan karena penggunaan teknologi mampu mempengaruhi eksistensi dan kemajuan dalam pengambilan keputusan pada instansi itu sendiri. Banyak cara untuk memanfaatkan perkembangan teknologi ini salah satunya dengan menggunakan komputer sebagai media input, pengolahan, penyimpanan, dan penyajian data ataupun informasi kepada pengguna. Dengan teknologi komputer, pengguna dapat meminimalisasi kesalahan dalam hal pengolahan data karena kinerja komputer dikendalikan oleh program yang bekerja secara otomatis.

Sekretariat DPRD kabupaten Musi Rawas sendiri adalah perpanjangan tangan Pemerintah kabupaten, sebagai Organisasi Perangkat Daerah yang mempunyai tugas utama yakni memfasilitasi tugas fungsi dan wewenang DPRD, sehingga

erat kaitannya keaktifan kinerja DPRD didukung oleh Sekretariat DPRD Fungsi sekretariat DPRD sebagai perpanjangan suara rakyat tentunya membutuhkan adanya rapat internal terkait keputusan- keputusan yang diambil. Setelah adanya rapat internal tentunya membutuhkan arsip data yang sangat rahasia agar data terjamin keamanannya.

Sistem informasi arsip surat ini bertujuan mengubah cara penyimpanan surat dengan cara mengurangi penggunaan kertas (*paperless*). Sistem informasi ini dibuat dengan menggunakan aplikasi *sublime*, bahasa pemrograman menggunakan PHP, Xampp digunakan untuk menjalankan *web server*, MySQL digunakan untuk pengelolaan *database*. Model alur hidup yang digunakan adalah *extreme programming*, sedang pengujian unit menggunakan *blackbox testing*. Dengan adanya penyimpanan surat secara *paperless*, kesalahan yang terjadi selama ini dapat diminimalisasi. Tujuan pembuatan aplikasi ini untuk membuat suatu sistem informasi yang mengolah data arsip surat sehingga lebih mudah dalam penggunaannya [1].

Arsip adalah rekaman kegiatan dalam berbagai bentuk dan media yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan dan organisasi maupun perseorangan. Selama ini di sekretariat DPRD kabupaten Musi Rawas utara dalam melakukan pengarsipan surat keputusan hasil rapat tertutup masih manual dengan memasukkan kedalam rak atau berkas surat sehingga rentan terjadinya kehilangan data atau kerusakan data dan terjamin isi surat keputusan tersebut [2].

Jadi untuk menjaga keamanan data dan menghindari kebocoran data dapat dilakukan berbagai cara salah satunya yaitu dengan melakukan kriptografi. Kriptografi yakni suatu cabang ilmu yang mengajarkan teknik-teknik yang mempunyai hubungan aspek-aspek yang ada dalam keamanan informasi. Pada kriptografi ini terdapat proses enkripsi dan dekripsi. Enkripsi merupakan proses yang mengganti sebuah kode dari yang dapat di mengerti dirubah menjadi kode yang tidak dapat dimengerti oleh pembaca deskripsi.

Penelitian terkait dengan arsip data yang pernah dilakukan oleh peneliti terdahulu. Tujuan dari penelitian ini adalah untuk mengetahui prosedur pengelolaan arsip pada kantor Wali Nagari Air Dingin di Kabupaten Solok. Berdasarkan hasil pengamatan pada pengelolaan arsip di Wali Nagari Air Dingin meliputi pencatatan surat masuk dan surat keluar dilakukan dengan cara manual, penyimpanan dan pemeliharaan arsip yang kurang baik, tempat penyimpanan arsip yang tidak terawat dan sulit untuk pencarian arsip. Sehingga perlu adanya sistem informasi untuk pengelolaan arsip, sistem informasi arsip dibangun

dengan menggunakan bahasa pemrograman PHP dan framework CodeIgniter berbasis web. [3]

Dalam penelitian lainnya terkait keamanan data arsip, Keamanan dokumen pada Klinik Dr. H. Hartono sangatlah penting seperti data rekam medik pasien. Rekam medik merupakan sebuah rekaman kesehatan yang memuat kumpulan dokumen-dokumen penting berkaitan dengan identitas, hasil anamnesis, hasil pemeriksaan fisik dan catatan segala kegiatan para tenaga kesehatan pada waktu ke waktu. Dokumen tersebut merupakan dokumen yang bersifat rahasia, jika dokumen rekam medik sampai jatuh ke tangan orang yang tidak bertanggung jawab, maka ada pihak yang dirugikan dalam insiden tersebut. Dari kebutuhan tersebut diperlukan suatu aplikasi pengamanan dokumen secara elektronik (E-Arsip) dengan melakukan penyandian informasi atau pesan yang akan dikirimkan melalui media pengiriman surat elektronik (e-mail) dengan cara mengimplementasikan 2 (dua) algoritma kriptografi yaitu RSA dan Elgamal [4]

Penelitian terkait implementasi algoritma SHA512 pernah dilakukan oleh peneliti terdahulu. Penelitian ini bertujuan untuk merancang dan membangun suatu aplikasi keamanan data/kriptosistem dan mengimplementasikan algoritma Rivest Shamir Adleman (RSA) dan fungsi hash SHA-512 ke dalam kriptosistem tersebut serta data digital yang digunakan adalah file bertipe dokumen (.doc/.docx dan .pdf), file bertipe teks (.txt), dan file bertipe audio (.mp3 dan .wav). Tahapan penelitian yang dilakukan meliputi persiapan dan pengumpulan data, analisis kebutuhan, analisis proses, perancangan sistem, implementasi dan pengujian, serta evaluasi hasil. Hasil dari penelitian ini adalah kriptosistem yang dapat melakukan proses enkripsi dan dekripsi dengan baik sehingga memenuhi aspek-aspek keamanan dari kriptografi yaitu kerahasiaan, integritas data, otentikasi dan penyangkalan [5].

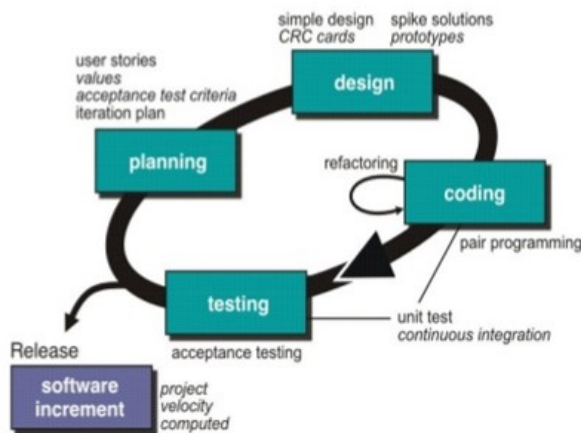
Dalam Penelitian ini menguraikan proses pengamanan untuk mendeteksi keaslian tanda tangan digital pada file video dengan menggunakan Metode SHA-512 dalam bentuk pendeteksian tanda tangan digital pada file video yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat dirubah atau dimodifikasi oleh orang yang tidak berhak atau orang yang tidak berkepentingan. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan penipuan, pemalsuan, *hoax*, atau-pun penyalahgunaan tanda tangan digital pada file video[6].

Untuk mengatasi permasalahan yang ada, maka dibutuhkan aplikasi berbasis *website* terkait pengarsipan berita acara hasil sidang yang dapat dilakukan secara *online* namun terjamin keamanan datanya.

2. METODE PENELITIAN

2.1. Metode *Extreme Programming*

Dalam mengembangkan suatu aplikasi terdapat beberapa metode yang digunakan, dalam penelitian ini digunakan metode *Extreme Programming (XP)*. Skema metode *extreme programming* terlihat pada gambar 1 berikut.

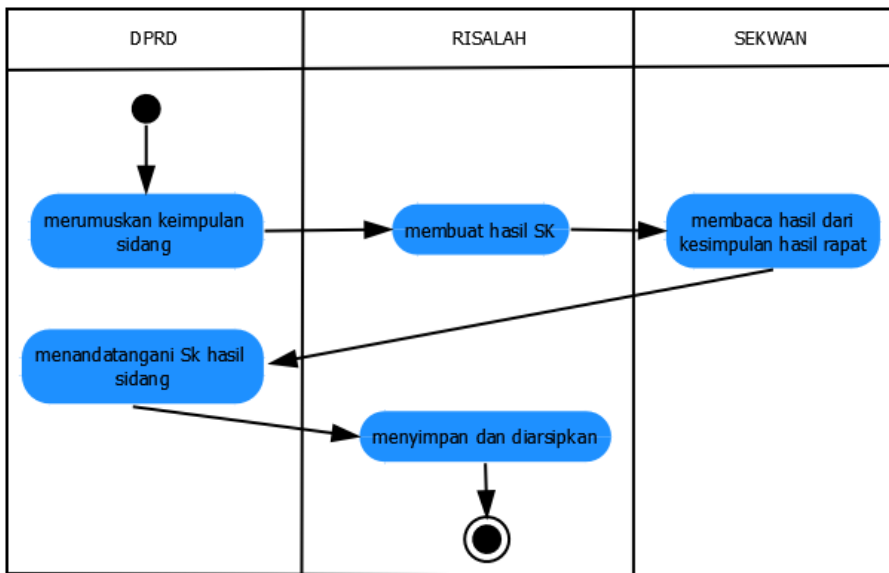


Gambar 1. Skema Metode *Extreme Programming*

Adapun tahapan dalam pembuatan aplikasi *point of sales* toko Azura Lubuklinggau berbasis *web* dengan XP adalah sebagai berikut:

1. *Planning* (Perencanaan)

Alur proses yang sedang berjalan, ketika terjadinya rapat maka yang memutuskan hasil sidang yaitu pihak DPRD yang di setuju paling dikit 2/3 dari jumlah anggota DPRD yang hadir. Sedangkan Risalah membuat surat keputusan yang telah disahkan oleh pihak DPRD. Dan surat keputusan yang telah disahkan akan di bacakan oleh sekwan dan DPRD menandatangani surat keputusan sidang dan akan di arsipkan oleh Risalah. Adapun sistem yang berjalan selama ini di kantor DPRD kab. Musi Rawas terkait keputusan sidang dilihat pada *activity diagram* berikut:



Gambar 2. Activity Diagram Sistem yang Berjalan

2. Design (Perancangan)

Dalam melakukan pemodelan sistem pada penelitian ini menggunakan *Unified Modelling Language (UML)* yang terdiri dari beberapa diagram antara lain *Use-Case Diagram*, *Activity Diagram*, *Sequence Diagram* dan *Class Diagram*.

3. Coding (Pengkodean)

Tahapan ini merupakan bentuk implementasi dari perancangan model sistem yang telah dibuat kedalam kode program yang menghasilkan suatu bentuk *prototype* dari aplikasi yang dibuat. Dalam pembuatan aplikasi keamanan SK hasil sidang menggunakan Bahasa pemrograman PHP yang dikombinasikan dengan CSS Bootstrap, Javascript dan Algoritma SHA512. Dalam mengimplementasikan *database* menggunakan *MySQL*.

4. Testing (Pengujian)

Metode yang digunakan dalam melakukan pengujian terhadap keamanan hasil sidang SK adalah metode pengujian *blackbox*.

5. Software Increment (Peningkatan Perangkat Lunak)

Tahapan ini merupakan tahapan mengembangkan sistem atau aplikasi yang telah dibuat secara bertahap yang dilakukan setelah sistem diimplementasikan oleh pihak DPRD Kab. Musi Rawas dengan menambahkan layanan atau fitur yang dibutuhkan oleh sistem kedepannya.

2.2. Perhitungan Algoritma SHA-512

Fungsi hash SHA-512 merupakan fungsi yang menghasilkan message digest ukuran 1024 bit. Terdapat 80 putaran dalam fungsi ini. Untuk melakukan padding bit dilakukan dengan cara yang sama dengan SHA-1

SHA-1 menggunakan urutan fungsi logika yang dilambangkan dengan f_0, f_1, \dots, f_{79} . Untuk masing-masing f_t , dimana $0 \leq t < 79$ akan menghasilkan output sebanyak 32 bit.

Contoh kasus pada proses ini dijelaskan yaitu file SK PDF. Cara pengambilan nilai data file aplikasi hanya diambil sebanyak 24 byte atau 48 karakter heksa desimal dan di konversi ke biner sebagai sampel metode, yang berguna untuk mengetahui nilai biner berikut:

0000001C6674797069736F6D000000206973

6F6D69736f3

- a. Penambahan bit-bit pengganjal dan nilai panjang pesan semula dari data yang digunakan dan diubah ke biner

Heksadesimal: 0000 001C 6674 7970 6973 6F6D 0000 0200
697 36F6D

6973 6f32 Data dalam biner: 00000000 00000000 00000000
00011100

01100110 01110100 01111001 01110000 01101001
01110011 01101111

01101101 00000000 00000000 00000010 00000000
01101001 01110011

01101111 01101101 01101001 01110011
01101111 0110010

Data sebanyak 24 byte di atas diketahui 192 bit, untuk mencukupi 1024 bit ditambah bit-bit pengganjal (padding bits) sebanyak 824 dan 8 bit, karena pada SHA-2 memproses blok-blok bit yang berjumlah 120 blok atau 1024 bit. Bit pengganjal yang ditambahi dimulai bit 1 diikuti bit 0 selebihnya hingga urutan bit 979 Untuk 8 bit terakhir menyatakan jumlah karakter dalam notasi biner yaitu 128 = 10000000

Berikut ini adalah urutan blok-blok bit setelah ditambahkan :

00000000 00000000 00000000 00011100 01100110 01110100 01111001
01110000 01101001 01110011 01101111 01101101 00000000 00000000
00000010 00000000 01101001 01110011 01101111 01101101 01101001
01110011 01101111 00110010 01101101 01110000 00110100 00110001
00000000 00000000 00000000 00001000 01100110 01110010 01100101
01100101 00000000 10011000 10011011 00010000 01101101 01100100
01100001 01110100 00000000 00000000 00000001 10110011 00000000
00010000 00000111 00000000 00000000 00000001 10110110 00010000
01100000 01000101 10000010 11101000 01110110 00001111 10000111

```
11111111 10111010 10001100 00000001 01110111 00110001 11011000
00111110 00011111 11111110 11101101 10000000 00101110 11100001
10110000 01110010 00011111 10000011 11000001 11111111 11010110
11001101 00000110 00100101 01111011 01110010 00100100 10000111
01001101 00000011 00000110 10100110 00001011 01100001 00010011
00010010 01000011 10100110 10000001 10000011 01010011 00001111
00001000 10010110 00000001 01101100 00000111 00111100 10100000
10000001 01000001 10001010 11000100 01110000 01100000 11010001
10000000
```

Bit yang bercetak tebal adalah bit dari plainteks file video, bit 1 pada urutan ke 193 yang bercetak tebal adalah awal dari bit pengganjal dan diikuti bit-bit 0 dan 8 bit terakhir bercetak tebal adalah bit yang menyatakan jumlah 128.

b. Inisialisasi Penyangga Nilai *Hash Message Digest* (MD)

Penyangga SHA-512 terdiri dari delapan yang setiap penyangga memiliki panjang 64 bit, berarti total 512 bit yaitu 8×64 , dan dalam notasi HEX yaitu:

A = 6a09e667f3bcc908

B = b67ae8584caa73b

C = 3c6ef372fe94f82b

D = a54ff53a5f1d36f1

E = 51e527fade683d1

F = 9b05688c2b3e6c1f

G = 1f83d9abfb41bd6b

H = 5be0cd19137e2179

Inisialisasi penyangga dalam biner, yaitu:

A = 6 a 0 9 e 6 6 7 f 3 b c c 9 0 8

= 0110 1010 0000 1001 1110 0110 0110 0111 1111 0011
1011 1100 1100 1001 0000 1000

B = b b 6 7 a e 8 5 8 4 c a a 7 3 b

= 1011 1011 0110 0111 1010 1110 1000 0101 1000 0100 1100
1010 1010 0111 0011 1011

C = 3 c 6 e f 3 7 2 f e 9 4 f 8 2 b

= 0011 1100 0110 1110 1111 0011 0111 0010 1111 1110 1001
0100 1111 1000 0010 1011

D = a 5 4 f f 5 3 a 5 f 1 d 3 6 f 1

= 1011 0101 0100 1111 1111 0101 0110 1011 0101 1111 0001
1101 0110 1011 1111 0001

E = 5 1 0 e 5 2 7 f a d e 6 8 2 d 1

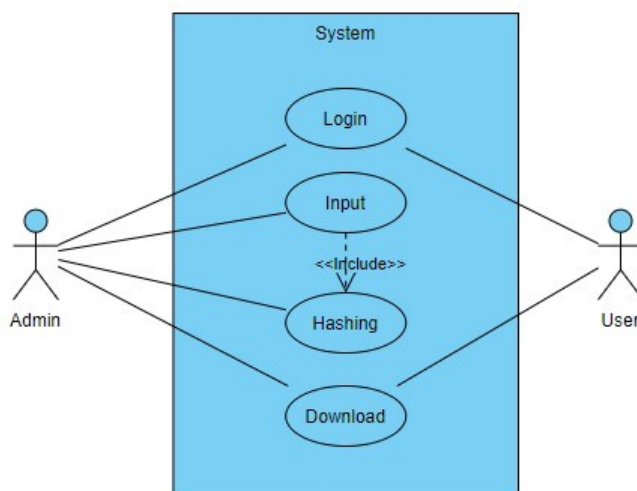
= 0101 0001 0000 1110 0101 0010 0111 1111 1010 1101 1110
0110 1000 0010 1101 0001

$F = 9b05688c2b3e6c1f$
 $= 1001\ 1011\ 0000\ 0101\ 0110\ 1000\ 1000\ 1100\ 0010\ 1011\ 0011$
 $1110\ 0110\ 1100\ 0001\ 1111$
 $G = 1f83d9abfb41bd6b$
 $= 0001\ 1111\ 1000\ 0011\ 1101\ 1001\ 1010\ 1011\ 1111\ 1011\ 0100$
 $0001\ 1011\ 1101\ 0110\ 1011$
 $H = 5be0cd19137e2179$
 $= 0101\ 1011\ 1110\ 0000\ 1110\ 1101\ 0001\ 1001\ 0001\ 0011\ 0111$
 $1110\ 0010\ 0001\ 0111\ 1001$

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan Sistem

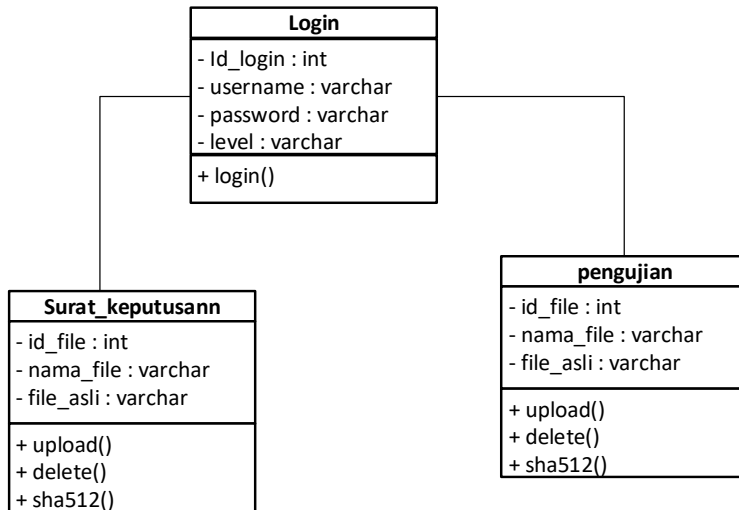
Sistem yang dibangun merupakan pembuatan sistem yang baru pada DPRD Kabupaten Musi Rawas dengan tujuan pengamanan dan integritas dokumen menggunakan algoritma SHA512. Dengan sistem baru, pihak bagian persidangan dapat menjaga integritas data dan memberikan kemudahan bagi para anggota dewan untuk melihat berita acara tanpa ada unsur manipulatif. Desain alur sistem arsip data di kantor DPRD kabupaten Musi Rawas digambarkan pada *use case* dan *class diagram* berikut.



Gambar 3. Use Case Diagram

Pada gambar 3, dijelaskan bahwa terdapat 2 (dua) aktor yang mengoperasikan sistem arsip surat di kabupaten Musi Rawas yakni admin dan *user*. Admin disini merupakan admin kantor DPRD kabupaten Musi Rawas sedangkan *user* disini

orang yang diberikan hak akses oleh admin untuk melihat atau mendownload data secara khusus. Admin dapat mengelola data arsip surat berupa input, edit dan hapus data yang kemudian data akan di *hashing* oleh sistem. *User* disini hanya bisa mendownload data arsip



Gambar 4. *Class Diagram*

3.2 Implementasi DBMS dan Antar Muka

1. Implementasi Basis Data Login, Data login disini digunakan untuk menyimpan data akses login admin dan *user*. Data login disini digunakan untuk masuk kedalam sistem arsip surat di *website* DPRD kabupaten Musi Rawas dengan level admin dan *user*. Pada basis data login terdapat field meliputi *id_login*, *username*, *password*, dan *level*. Berikut implementasi basis data login.

			<i>id_login</i>	<i>username</i>	<i>password</i>	<i>level</i>
<input type="checkbox"/>				1	admin	21232f297a57a5a743894a0e4a801fc3 admin
<input type="checkbox"/>				2	fentin	ee11cbb19052e40b07aac0ca060c23ee user
<input type="checkbox"/>				4	user2	ee11cbb19052e40b07aac0ca060c23ee user
<input type="checkbox"/>				5	user3	ee11cbb19052e40b07aac0ca060c23ee user

Gambar 5. Implementasi Basis Data Login

2. Implementasi Basis Data Pengujian, Data Pengujian disini digunakan untuk melakukan pengujian data apakah data file asli yang telah di upload dengan data uji sudah sesuai atau belum sesuai. Pada basis data pengujian terdapat field meliputi id_field, nama_file, file_asli, dan hasil. Berikut implementasi basis data pengujian :

	id_file	nama_file	file_asli	hasil
<input type="checkbox"/> Ubah Salin Hapus	85	4229f5717713cea343eed956be8f8c5654efa8140144fd1304...	fae989d0487771d257a19bba575cf1c04ddfd7bfe87a911a...	Tidak Sesuai
<input type="checkbox"/> Ubah Salin Hapus	86	6b2a3c9f7c73649e74725a890df5085359397e88f12208e228...	643c855e6a41c681fa7c58f355b851e410a20a767c92018a0d...	Sesuai
<input type="checkbox"/> Ubah Salin Hapus	87	dfc15c736210684ead2fc4e204e3124d4d109bf2a35b26eb46...	4783de9bdeda2da3a627b1386a15169fa209367efdc39eb3d4...	Sesuai

Gambar 6. Implementasi Data Pengujian

3. Implementasi Basis Data Surat Keputusan, Data Surat Keputusan digunakan untuk menyimpan data arsip surat yang dikelola oleh admin. Pada basis data surat keputusan terdapat field meliputi id_file, nama_file, dan keterangan. Berikut implementasi basis data surat keputusan:

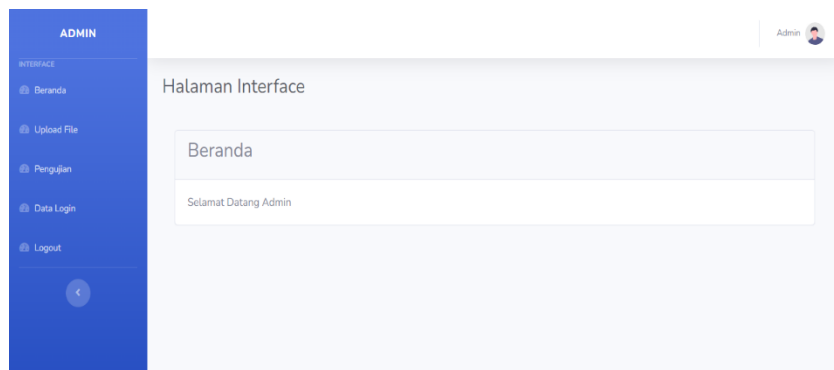
	id_file	nama_file	keterangan
<input type="checkbox"/> Ubah Salin Hapus	127	643c855e6a41c681fa7c58f355b851e410a20a767c92018a0d...	07-09-2022 13:28
<input type="checkbox"/> Ubah Salin Hapus	128	4783de9bdeda2da3a627b1386a15169fa209367efdc39eb3d4...	07-09-2022 14:47

Gambar 7. Implementasi Basis Data Surat Keputusan

3.3 Impementasi Interface/Antarmuka Sistem

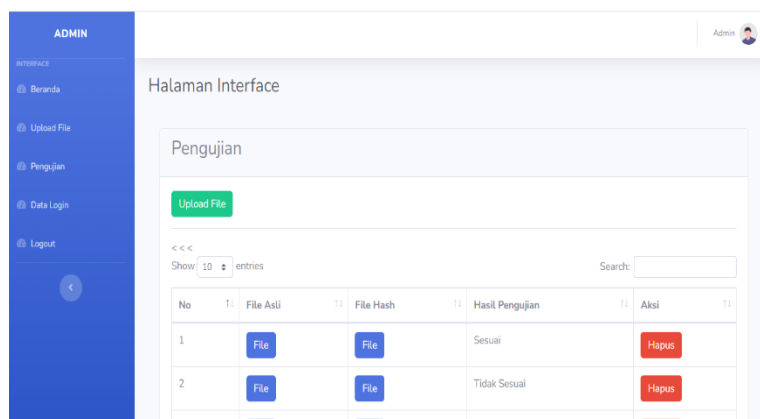
Model *interface* / antarmuka merupakan tahapan lanjutan dari perancangan bab selanjutnya. Model *interface* / antarmuka digunakan untuk menggambarkan mekanisme komunikasi antara pengguna (user) dengan sistem untuk membantu mengarahkan alur penelusuran. Berikut implementasi dari perancangan *interface* atau antarmuka aplikasi Keamanan Berita Acara Hasil Sidang menggunakan Algoritma SHA512 di DPRD Musi Rawas:

1. Implementasi Halaman Dashboard Admin, Halaman dashboard merupakan halaman yang akan tampil pertama kali ketika admin berhasil melakukan login ke dalam aplikasi. Halaman *dashboard* admin disini digunakan untuk mengelola data seperti kelola data arsip surat, pengujian data arsip dan data login untuk *user* untuk mendownload arsip data. Halaman dashboard admin dapat dilihat pada gambar 8 berikut:



Gambar 8. Implementasi Halaman Dashboard Admin

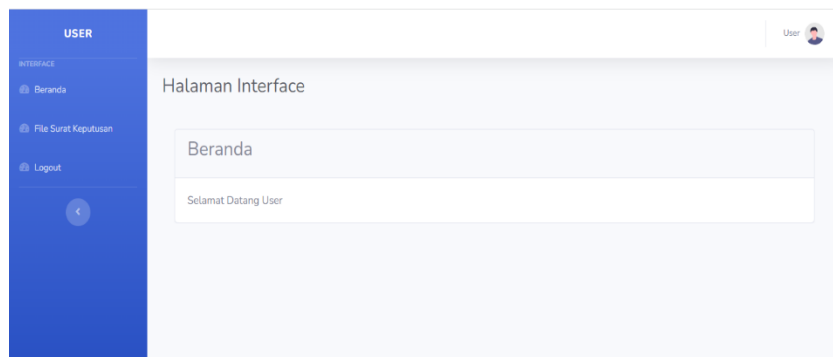
2. Implementasi Halaman Pengujian
Halaman pengujian merupakan halaman yang menampilkan data pengujian *hashing* dan digunakan untuk melakukan pengujian terhadap file yang akan di *hashing*. Pengujian dilakukan untuk melakukan pencocokan antara data file yang telah di upload sebelumnya dengan data uji yang diupload apakah sudah sesuai atau belum sesuai. Halaman Pengujian dapat dilihat pada gambar 9 berikut:



Gambar 9. Implementasi Halaman Pengujian

3. Implementasi Halaman *Dashboard User*

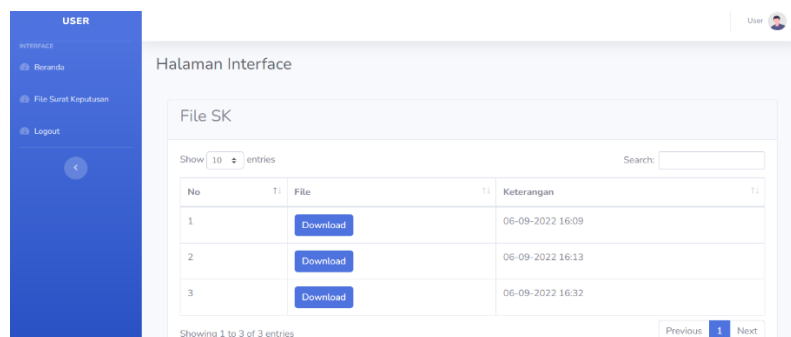
Halaman dashboard *user* merupakan halaman yang akan tampil pertama kali ketika user berhasil melakukan login dan berhasil berperan sebagai *user*. Halaman *user* disini hanya dapat melakukan *download* file arsip yang telah dimasukkan oleh petugas admin sebelumnya oleh admin DPRD kabupaten Musirawas. Halaman *dashboard user* dapat dilihat pada gambar 10 berikut:



Gambar 10. Implementasi Halaman Dashboard User

4. Implementasi Halaman File Surat Keputusan

Halaman file surat keputusan merupakan halaman yang terdapat pada *interface user* dan digunakan untuk melakukan *download* atau menyimpan data *file* arsip yang dimasukkan oleh admin kantor DPRD kabupaten Musi Rawas dan diamankan melalui proses *hashing* menggunakan algoritma SHA512. Halaman file surat keputusan dapat dilihat pada gambar 11 berikut:



Gambar 11. Implementasi Halaman File Surat Keputusan

4. KESIMPULAN

Berdasarkan hasil dari hasil uji coba dan aplikasi arsip surat berbasis web pada kantor DPRD, maka dapat disimpulkan

1. Dari gambaran secara umum penulis melakukan penelitian terhadap sistem arsip berita acara hasil sidang yang terjadi di kantor DPRD Kab.Musi Rawas, bahwasanya sistem yang digunakan masih secara manual atau masih menggunakan *paperless* sehingga tidak menjamin keamanan datanya.
2. Dengan adanya aplikasi ini agar dapat memudahkan sistem kerja proses arsip data dan terjaminnya keamanan data.
3. Metode pengembangan ini menggunakan metode *extreme programming*, karena dengan model ini memberi pendekatan pengembangan secara sekuen dan sistematis untuk pengembangan aplikasi dan dilakukan dengan model fase *one by one*, sehingga meminimalis kesalahan yang mungkin terjadi.

DAFTAR PUSTAKA

- [1] S. Saifudin and A. Y. Setiaji, "Sistem Informasi Arsip Surat (Sinau) Berbasis Web Pada Kantor Desa Karangsalam Kecamatan Baturraden," *EVOLUSI J. Sains dan Manaj.*, vol. 7, no. 2, pp. 15–21, 2019, doi: 10.31294/evolusi.v7i2.6751.
- [2] A. A. J. SinlaE, E. Ngaga, and S. D. B. Mau, "Rancang Bangun Kriptosistem untuk Pengamanan Data-data Digital," *J. Maklumatika*, vol. 5, no. May, pp. 64–75, 2018,
- [3] N. Firdaus and D. Irfan, "Rancang Bangun Sistem Informasi Arsip Berbasis Web Menggunakan Framework Codeigniter," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 8, no. 1, p. 44, 2020, doi: 10.24036/voteteknika.v8i1.107759.
- [4] S. J. Diah Anggraini, "Aplikasi E-Arsip Pengamanan Pesan Elektronik Berbasis Web dengan Mengimplementasikan Algoritma Kriptografi RSA dan Elgamal pada Klinik Dr. H. Hartono," *J. TICOM*, vol. 6, no. 3, 2018.
- [5] M. Ipdal, "Analisa Metode SHA-512 Untuk Tanda Tangan Digital Pada File Video," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 1, 2021.
- [6] D. Sinaga, "IMPLEMENTASI SHA512 PADA APLIKASI KRIPTOGRAFI FILE," *SENDI_U*, 2018.
- [7] R. A. Shalahuddin, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek, 3rd ed.* Bandung: Informatika, 2014.
- [8] R. Munir, *Algoritma Kriptografi Klasik*. 2014.
- [9] R. Sadikin, *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Andi, 2012.
- [10] M. Mundzir, *PHP Tutorial Book for Beginner*. Yogyakarta: Andi, 2014.
- [11] A. Kadir, *Pengenalan Sistem Informasi*. Yogyakarta: Andi, 2014.

- [12] H. Riyadli, A. Arliyana, and F. E. Saputra, "Rancang Bangun Sistem Informasi Keuangan Berbasis WEB," *J. Sains Komput. dan Teknol. Inf.*, vol. 3, no. 1, pp. 98–103, 2020, doi: 10.33084/jsakti.v3i1.1770.