Jurnal Elektronik Ilmu Komputer Udayana
Volume 10, No 2. November 2021

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengamanan Lontar Digital Dengan Tanda Tangan Digital Menggunakan Algoritma RSA

I Ketut Gede Suhartana[a1], I Gede Bendesa Aria Harta[a2], I Gusti Ngurah Anom Cahyadi Putra[b3], Cokorda Rai Adi Pramartha[b4], I Komang Ari Mogi[b5], Made Agung Raharja[b6]

[a]Program Studi Teknik Informatika, Jurusan Ilmu Komputer, Fakultas Matermatika dan Ilmu Pengetahuan Alam Universitas Udayana
Jalan Raya Kampus Unud, Badung, 08361, Bali, Indonesia
[1]ikg.suhartana@unud.ac.id
[2]ariaharta@gmail.com
[3]anom.cp@unud.ac.id
[4]cokorda@unud.ac.id
[5]arimogi@unud.ac.id
[6]made.agung@unud.ac.id

Abstract

Lontar merupakan peninggalan warisan karya budaya yang sumber dasar pembuatannya dari rontal atau daun tal berisi bukti-bukti segala catatan aspek kehidupan sejarah zaman dahulu yang meliputi nilai dari catatan sejarah, nilai agama, nilai filsafat, nilai pengobatan, nilai sastra dan ilmu dari pengetahuan lainnya sehingga kelestariannya perlu dijaga. Pengamanan lontar digital akan memudahkan dalam menjaga kelestarian suatu karya lontar agar tidak diubah atau dimanipulasi sedemikian rupa oleh pihak-pihak yang merugikan atau tidak bertanggung jawab, yang dimana lontar digital berformat PDF akan diberikan tanda tangan digital untuk menjaga keotentikan dokumen (Azdy ., 2016). Jadi dokumen yang ditanda tangani akan menjadi sangat sulit untuk dimodifikasi atau diubah oleh pihak lain, jika isi dari sebuah lontar digital diubah maka akan mengakibatkan tanda tangan digitalnya pun berubah. Berdasarkan penelitian yang dilakukan, dari hasil pengujian Pengamanan lontar digital dengan tanda tangan digital dengan menggunakan algoritma RSA didapatkan hasil pengujian dari RMSE (Root Mean Square Error) untuk hasil deskripsi dengan rata - rata 69.7794143. Semakin besar atau acak hasil deskripsi maka hasil deskripsi akan makin kompleks.

Keywords: *Tanda Tangan Digital, Algoritma RSA, RMSE, Lontar Digital.*

1. Pendahuluan

Lontar merupakan hasil dari produk budaya dan telah di akui menjadi suatu warisan dari budaya dunia. Pada kata lontar itu sendiri mempunyai hubungan dari sumber bahan dasar pembuatan lontar itu sendiri, yaitu dari daun rontal atau daun ental atau daun tal sebagai bahan dasarnya. Lontar yang digunakan sebagai produk untuk melestarikan suatu karya budaya yang sangat kaya makna dan arti telah menjadi citra dari tradisi didalam tengah-tengah peradaban pergaulan di dunia. Sehingga warisan dari catatan budaya yang berharga ini juga sudah memberikan catatan kelelulуhuran serta mentransmisikan sebuah karya keunggulan yang bersumber dari pemikiran orang yang telah menciptakan karya tersebut (Sawitri dkk., 2020). Dalam tradisi dari sebuah lontar juga dapat memiliki pengetahuan akan perjalanan dari sebuah sejarah yang penting serta panjang dan usia yang bertambah menua seiring dengan nilai sejarah, nilai agama, nilai filsafat, nilai pengobatan, nilai sastra, serta ilmu pengetahuan yang sangat tinggi. Jadi lontar pada sampai saat dalam bentuknya kini adalah merupakan catatan sejarah serta dianggap menjadi panduan dalam masyarakat yang mendukungnya jadi kelestariannya perlu dijaga.

Menurut Peraturan yang dikeluarkan oleh Gubernur Bali yang bernomor 80 Tahun 2018 mengenai penggunaan dan perlindungan sastra bali, Aksara dan bahasa dan untuk penyelenggaraan Bulan Bahasa Bali, yang dimana dipergunakan dalam menulis segala macam aspek kehidupan manusia yang sudah ada sejak dari zaman dahulu, pembuktian dari hal tersebut tersebut muncul dalam segala pembukuan purana, lontar, prasasti serta berbagai pembukuan catatan lain dalam mengisi budaya kearifan leluhur dari zaman dahulu serta, seni, dan juga tradisi (Redaksi9.com., 2019).

Untuk menjaga kelestarian suatu karya tersebut agar isi dari lontar tersebut tidak diubah atau dipalsukan oleh mereka yang sangat merugikan, penulis berinisiatif untuk menciptakan sebuah sistem pengamanan file lontar digital yang berformat file pdf dengan menggunakan tanda tangan digital. Jadi Tanda tangan digital merupakan mekanisme dari sebuah pengenalan tanda tangan yang menggunakan basis dari skema ilmu pengetahuan kriptografi. Untuk metode Tanda tangan digital diciptakan dari memanfaatkan fungsi ilmu kriptografi kunci publik. Tanda tangan digital biasanya digunakan agar dapat membuktikan keontetikan sebuah dari sebuah file dokumen. File dari dokumen yang sudah diberikan tanda tangan dipastikan akan berubah menjadi sangat sukar jika akan dimodifikasi oleh orang lain. Letak keamanan dari metode penandatanganan digital ini merupakan keontetikan dari penandatanganan digital tersebut, karena tanda tangan digital tidak dapat ditiru maupun dirubah, jadi jika isi dari sebuah dokumen sudah dirubah akan mengakibatkan tanda tangan digitalnya pun berubah (Ardiansyah dkk., 2018). Dalam penelitian ini, penulis menggunakan metode tanda tangan digital dengan algoritma RSA sebagai algoritma kunci publik, serta MD5 sebagai fungsi hashnya. Fungsi dari algoritma RSA dapat menghasilkan tingkat pengamanan yang sangat tinggi, dari fungsi perlindungan algoritma ini terdapat dalam sangat sulitnya mengfaktorkan angka non prima menjadi bilangan prima dalam memecahkan kunci dari algoritma tersebut (Ginting dkk., 2015). Algoritma ini nantinya akan digunakan sebagai algoritma kunci publik dalam penelitian ini. Lalu fungsi hash yang akan digunakan adalah fungsi hash MD5 karena nantinya saat pesan dihash, maka akan menghasilkan message digest (Hutasuhut, B. K., 2019). Hal ini sudah cukup meyakinkan penulis bahwa fungsi hash yang digunakan dalam penelitian ini merupakan fungsi hash yang sangat baik.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2. Metode Penelitian

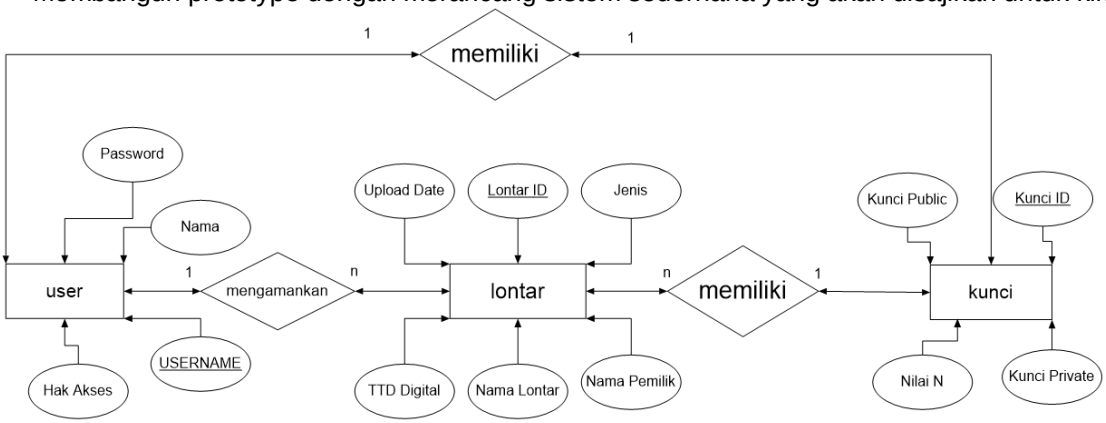
Metode prototype adalah suatu metode yang dimana dalam pengembangan perangkat lunak merupakan metodelogi siklus dari sebuah sistem yang dibuat berdasarkan dari model kerja konsep. Dalam metodelogi prototype, perangkat lunak yang sudah dihasilkan kemudian akan dipresentikan kepada klien untuk memberikan masukan serta kritik, sehingga software yang dihasilkan sesuai dengan keinginan dan kebutuhan klien. Berikut adalah siklus hidup dalam pengembangan prototyping :

2.1. Pengumpulan Kebutuhan

Pengembang serta Klien bersama-sama membuat konsep dari software yang akan dibuat, mengidentifikasikan kebutuhan program yang nantinya dibuat

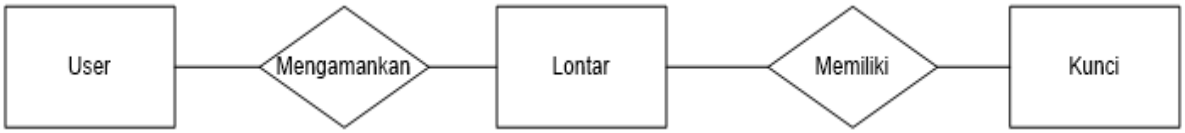
2.2. Membuat Prototype

Membangun prototype dengan merancang sistem sederhana yang akan disajikan untuk klien



Gambar 1. Entity Relationship Diagram

Gambar di atas menunjukan perancangan sistem menggunakan ERD. Di dalam ERD tersebut terdapat 3 buah entitas antara user, lontar dan kunci. User dan lontar dihubungkan dengan relasi mengamankan. Mengamankan bisa diartikan enkripsi dan verifikasi. Pada entitas lontar dan kunci terdapat atribut user id yang merupakan foreign key yang berasal dari user yang digunakan dalam enkripsi dan verifikasi sebuah lontar.



Gambar 2. konseptual Data Model

Gambar diatas merupakan konsep database, terdapat 3buah entitas antara lain user, lontar, kunci yang saling berhubungan.

2.3. Evaluasi Prototyping

Pada tahap ini klien menilai apakah prototyping yang sudah dibuat cocok dengan kebutuhan dan keperluan klien. Bila belum cocok proses prototype mengulangi proses langkah sebelumnya yaitu

1,2 dan kembali ke tahap 3. Tapi jika sudah cocok dengan keinginan klien maka selanjutnya langkah proses akan dikerjakan

2.4. Pengkodean Sistem

Pada tahapan saat ini prototyping yang sudah dibuat serta sudah disepakati dan dikodekan menggunakan pemrograman yang klien inginkan.

2.5. Pengujian Sistem Prototyping

Selanjutnya sistem yang telah menjadi software yang akan digunakan, selanjutnya software akan diuji terlebih dahulu sebelum akan digunakan untuk meminimalisir kesalahan pada software. Pengujian pada sistem akan menggunakan RMSE (Root Mean Square Error) untuk mengetahui kualitas dan perbedaan hasil dari sistem yang dibuat, proses perhitungan dilakukan sebagai berikut :

$$\frac{1}{n}\sqrt{\sum_{i=1}^{n}(zi' - zi)^2}$$

Gambar 3. RMSE

Keterangan :
n = jumlah total inputan pesan
zi'= nilai pesan hasil (chipertext)
zi = nilai pesan asli (Plaintext)
Semakin besar nilai RMSE yang dihasilkan dari dua nilai yang diukur, maka semakin besar perbandingan kemiripan antar kedua teks tersebut. jadi akan semakin aman hasil dari pengujian RMSE tersebut. dengan menggunakan pengujian RMSE dibuktikan hasil kualitas dan keamanan dari enkripsi dan dekripsi dari algoritma yang sudah diterapkan.

2.6. Evaluasi Sistem

Ditahapan ini klien akan menilai dari sistem yang sudah selesai dibuat dengan persis diharapkan. Bila tidak, selanjutnya pengembang dapat mengulangi proses langkah 4 dan 5. Namun bila sesuai maka proses akan dilanjutkan ke tahapan selanjutnya.

2.7. Menggunakan Sistem

Dalam tahap ini software yang sudah jadi dan diuji oleh klien sudah siap untuk pakai.

3. Hasil dan Pembahasan

Pengimplementasian sistem pengamanan file lontar digital mencakup lingkup perangkat lunak dan perangkat keras. Dimana implementasi pada sistem dibangun menggunakan aplikasi berbasis desktop dengan menggunakan Bahasa pemrograman Phyton. Berikut spesifikasi dari perangkat keras yang penulis gunakan yaitu:
1. Proccesor Intel Core I7 2,60 Ghz
2. RAM 4 GB
3. HDD 1 TB
Berikut untuk penggunaan perangkat lunak yang dipergunakan oleh penulis:
1. Spyder
2. Sistem Operasi Windows 10

3.1 Pengujian RMSE

Pada pengujian ini dilakukan tahapan uji kemiripan data saat sudah dienkripsi dan sebelum data dienkripsi pada program. Pengujian ini menggunakan RMSE (Root Mean Square Error) agar dapat mengetahui perbedaan dan kualitas hasil dari pengujian dari program yang sudah dibuat. Hasil dari enkripsi yaitu chipertext dan pesan asli yaitu plaintext akan dihitung nilainya dengan mengubah karakter

p-ISSN: 2301-5373
e-ISSN: 2654-5101

yang dienkripsi atau sebelum dienkripsi tersebut dengan menjadi sebuah bilangan ASCII. Jumlah dari karakter yang akan digunakan adalah plaintext sebanyak 12 buah dan chipertext sebanyak 12 buah. Karakter chipertext dan karakter plaintext akan diubah terlebih dahulu ke dalam bilangan ASCII kemudian dilakukan proses perhitungan sesuai dengan rumus. Maka akan didapatkan nilai berikut.

Tabel 1. Tanda Tangan Digital

NO	Plaintext	Chipertext
1	6322d27e8e76	116168037337
2	e45f9aae5f1f	458356725442
3	57295b3b20bd	109688044126

NO	$\sum(Zi' - Zi)^2$ Data I	$\sum(Zi' - Zi)^2$ Data II	$\sum(Zi' - Zi)^2$ Data III
1	25600	117649	32041

Tabel 2. Hasil selisih RMSE

Keterangan :

Data I = Plaintext 1 = WzQ0NCwgMTQ0MCwgNDQ0LCA5

Data II = Plaintext 2 = WzE0MjYsIDYxMSwgNDQ0LCAz

Data III = Plaintext 3 = WzEwNzIsIDE0MjYsIDg3NCwg

Adapun perhitungan dari RMSE tersebut adalah

$\sum_{i=1}^{n}$ $(zi' - zi)^2$ = ∑(Zi' – Zi) Data I + ∑(Zi' – Zi) Data II + ∑(Zi' – Zi) Data III

= 25600 + 117649 + 32041

= 175290

$\frac{1}{n}\sqrt{\sum_{i=1}^{n} (zi' - zi)2}$ $= \frac{1}{n}\sqrt{175290}$

$= \frac{1}{36}\sqrt{175290}$

$= \sqrt{\frac{175290}{36}}$

$= \sqrt{4869.1667}$

= 69.7794143

Nilai hasil RMSE dapat berkisar dari 0 nilai terendah sampai dengan nilai ∞, yang dimana dalam penelitian ini didapat hasil dengan rata - rata 69.7794143. Dari hasil tersebut dapat membuktikan bahwa terdapat perbedaan antara chipertext dan plaintext. Dengan mendapatkan nilai tersebut yang bila hasil

deskripsi makin besar atau acak maka deskripsi makin kompleks, sehingga dibuktikan bahwa tingkat keamanan algoritma RSA baik diterapkan pada program sistem tanda tangan digital.

4. Kesimpulan

Hasil dari penelitian yang telah dikerjakan oleh penulis, diperoleh beberapa rangkuman beberapa hal dalam penelitian yang berjudul Pengamanan Lontar Digital Dengan Tanda Tangan Digital Menggunakan Algoritma RSA :

A. Pembuatan aplikasi penandatanganan lontar digital yang berformat file PDF menggunakan metode Rivest Shamir Adleman (RSA) dapat dilakukan dengan cara mengaplikasikan enkripsi RSA terhadap text yang dihasilkan dari pembacaan file PDF lontar digital dari sistem. Dengan menyimpan encrypted message yang dihasilkan beserta public key dari proses enkripsi, aplikasi dapat memverifikasi keaslian file lontar digital yang diinputkan oleh user.

B. Untuk memverifikasi file lontar yang sudah ditanda tangani dengan metode RSA, aplikasi akan membaca file PDF yang diinputkan user kemudian membandingkan dengan hasil dekripsi dari file tersebut yang disimpan di database. Jika kedua teks tersebut sama, maka keaslian dari file tersebut dianggap valid.

C. Dilihat dari hasil pengujian menggunakan RMSE dapat dibuktikan perbedaan dari plantext dan chipertext memiliki nilai RMSE yang tinggi yaitu 69.77941433, dari hal tersebut dapat disimpulkan bahwa plaintext dan chipertext memiliki perbedaan karakter yang berbeda dan setelah diverifikasi, file pdf lontar digital masih akan membandingkan lagi dengan message digestnya. File lontar digital yang message digestnya berbeda dapat disimpulkan bahwa data file tersebut adalah palsu. Hal tersebut dikarenakan metode hash memiliki sifat apabila sebuah karakter diubah maka message diegest yang dihasilkan akan berbeda.

Referensi

[1] Achmad Ardiansyah, & Mepa Kurniasih. (2018). Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit. Jurnal Teknologi Informasi Vol. XIII Nomor 3 November 2018 ISSN: 1907-2430.

[2] Albert Ginting, R. Rizal Isnanto, & Ike Pertiwi Windasari. (2015). Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi dan Sistem Komputer. Vol.3, No.2, April 2015 (e-ISSN: 2338-0403).

[3] Dewa Ayu Dian Sawitri, & Ni Ketut Supasti Dharmawan. (2020). Perlindungan Transformasi Karya Cipta Lontar Dalam Bentuk Digitalisasi. Jurnal Hukum Kenotariatan Vol. 5 No. 2 Agustus 2020 P-ISSN: 2502-8960, E-ISSN: 2502-7573.

[4] Hutasuhut, B. K. (2019). Analisis Rancangan Model Digital Signature Dengan Kombinasi Algoritma MD5, Algoritma RSA Untuk Menguji Keaslian Data Dengan Akurat. Program Studi S2 Teknik Informatika Fakultas Ilmu Komputer Dan Teknologi Informasi Universitas Sumatera Utara Medan.

[5] Redaksi9.com. (2019, Desember 1). Pergub Nomer 80 Tahun 2018 untuk Memuliakan Aksara Bali, Tidak Bertentangan UU. Retrieved juni 21, 2021, from https://www.redaksi9.com/read/1361/Pergub-Nomor-80-Tahun-2018-untuk-Memuliakan-Aksara-Bali--Tidak-Bertentangan-UU.html#!

[6] Rezania Agramanisti Azdy. (2016). Tanda Tangan Digital Menggunakan Algoritme Keccak dan RSA. JNTETI, Vol. 5, No. 3, Agustus 2016.s