Hello World
Jurnal Ilmu Komputer
https://jurnal.ilmubersama.com/index.php/hello_world

Cryptography

Pengamanan Elektronik Arsip (E-Arsip) pada Kantor Desa Buntu Bedimbar Menggunakan Algoritma Rivest Shamir Adleman (RSA)

Ahmad Dani Dalimunthe [1], Rachmat Aulia [2], Oris Krianto Sulaiman [1]*

[1] *Fakultas Teknik, Program Studi Teknik Informatika, Universitas Islam Sumatera Utara, Medan, Indonesia*
[2] *Fakultas Teknik, Program Studi Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia*

INFORMASI ARTIKEL

Diterima Redaksi: 15 Oktober 2024
Revisi Akhir: 26 Maret 2025
Diterbitkan *Online*: 27 Maret 2025

KATA KUNCI

Arsip Data
Kantor Desa
Rivest Shamir Adleman (RSA)
Pengamanan Surat

KORESPONDENSI (*)

Phone: +62 812-6766-0329
E-mail: ahmaddanidalimunthe3468@gmail.com

A B S T R A K

Perkembangan teknologi khususnya teknologi komputer telah mengalami kemajuan yang sangat pesat. Perkembangan teknologi tersebut tidak lepas dari peran manusia yang setiap saat harus memperbaiki dan mencari inovasi baru agar teknologi tersebut dapat digunakan untuk membantu pekerjaan manusia. Namun pada kenyataannya masih banyak perusahaan atau organisasi yang belum menggunakan teknologi komputer sebagai alat bantu pekerjaan, seperti sistem Pengarsipan yang penulis jadikan kasus dalam pembuatan penelitian ini yang masih menggunakan cara manual pada Kantor Desa Buntu Bedimbar. Sistem manual seperti itu menyulitkan petugas ketika akan mencari surat yang diinginkan karena harus mencari data satu persatu. Kearsipan merupakan bagian pekerjaan dari suatu institusi yang sangat penting, informasi tertulis yang tepat harus tersedia apabila diperlukan agar suatu institusi dapat memberikan pelayanan yang efektif. Tujuan pada penelitian ini yaitu pembuatan aplikasi yang mampu melakukan suatu kegiatan seperti pengarsipan data secara elektronik dan melakukan pengamanan data dengan menggunakan Algoritma Rivest Shamir Adleman (RSA). Sistem ini di rancang menggunakan Software PHP dan Database XAMPP.

PENDAHULUAN

Perkembangan teknologi pada saat ini khususnya teknologi komputer telah mengalami kemajuan yang sangat pesat. Perkembangan teknologi tersebut tidak lepas dari peran manusia yang setiap saat harus memperbaiki dan mencari inovasi baru agar teknologi tersebut dapat digunakan untuk membantu pekerjaan manusia.

Kita tahu bahwa teknologi komputer pada saat ini telah banyak digunakan di berbagai organisasi, baik organisasi besar maupun kecil. Teknologi komputer dimanfaatkan sebagai alat bantu untuk mempermudah pekerjaan dari perusahaan atau organisasi tersebut. Namun pada kenyataannya masih banyak perusahaan atau organisasi yang belum menggunakan teknologi komputer sebagai alat bantu pekerjaan, seperti pengarsipan data yang masih dilakukan secara manual oleh kebanyakan instansi pada saat ini. Dan itu akan memperlambat kinerja pegawai dalam melakukan pengarsipan secara manual.

Elektronik Arsip (E-Arsip) adalah sistem pengelolaan arsip yang menggunakan teknologi digital untuk menyimpan, mengelola, dan mengakses dokumen atau informasi. E-Arsip memungkinkan organisasi untuk menyimpan data dalam format elektronik, menggantikan arsip fisik yang seringkali memakan banyak ruang dan sulit diakses.

Melakukan pengarsipan data surat masuk dan surat keluar tentunya harus mempunyai keamanan yang sangat kuat, dan data-data tersebut harus memiliki kunci yang akan menjaga keamanan dan kerahasiaan informasi seperti kunci publik dan

https://doi.org/10.56211/helloworld.v3i4.670

kunci privat. Menggunakan dua kunci memungkinkan banyak orang untuk mengenkripsi data untuk satu penerima tanpa memberikan akses ke kunci privat, menjaga dan kontrol akses. Untuk melakukan enkripsi data tersebut dengan cara mengimplemetasikan algoritma *Rivest Shamir Adleman*. *Algorima Rivest Shamir Adleman* adalah algortima kriptografi yang paling banyak digunakan untuk mengamankan data karena pada algoritma RSA memiliki standar yang luas digunakan, sehingga mudah di integrasikan dengan berbagai sistem dan aplikasi.
Cara kerja algoritma RSA dalam aplikasi E-Arsip ini dengan menggunakan dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi data, sementara kunci pribadi digunakan untuk mendekripsi data.
Tujuan dari aplikasi ini yaitu untuk mengamankan surat-surat yang ada pada kantor Desa Buntu Bedimbar serta memberikan kemudahan bagi para pegawai untuk pengarsipan surat-surat yang ada pada kantor Desa Buntu Bedimbar.

TINJAUAN PUSTAKA

Arsip

Arsip merupakan salah satu sumber informasi penting yang dapat menunjang proses kegiatan administrasi maupun birokrasi. Sebagai rekaman informasi dari seluruh aktivitas organisasi, arsip berfungsi sebagai pusat ingatan, alat bantu pengambilan keputusan, bukti eksistensi organisasi dan untuk kepentingan organisasi yang lain [1]. Arsip juga merupakan naskah tertulis yang didalamnya memuat keterangan-keterangan penting [2].

Website

Website merupakan sebuah kumpulan halaman-halaman web beserta file-file pendukungnya, seperti file gambar, video, dan file digital lainnya yang disimpan pada sebuah web server yang umumnya dapat diakses melalui internet [3].
Website merupakan salah satu sumber daya teknologi yang berkembang pesat. Saat ini, informasi web didistribusikan lebih dekat dan mudah, yang memungkinkan suatu teks, gambar ataupun objek yang lain menjadi acuan dasar untuk membuka halaman halaman web yang lain [4].

Pengertian Database

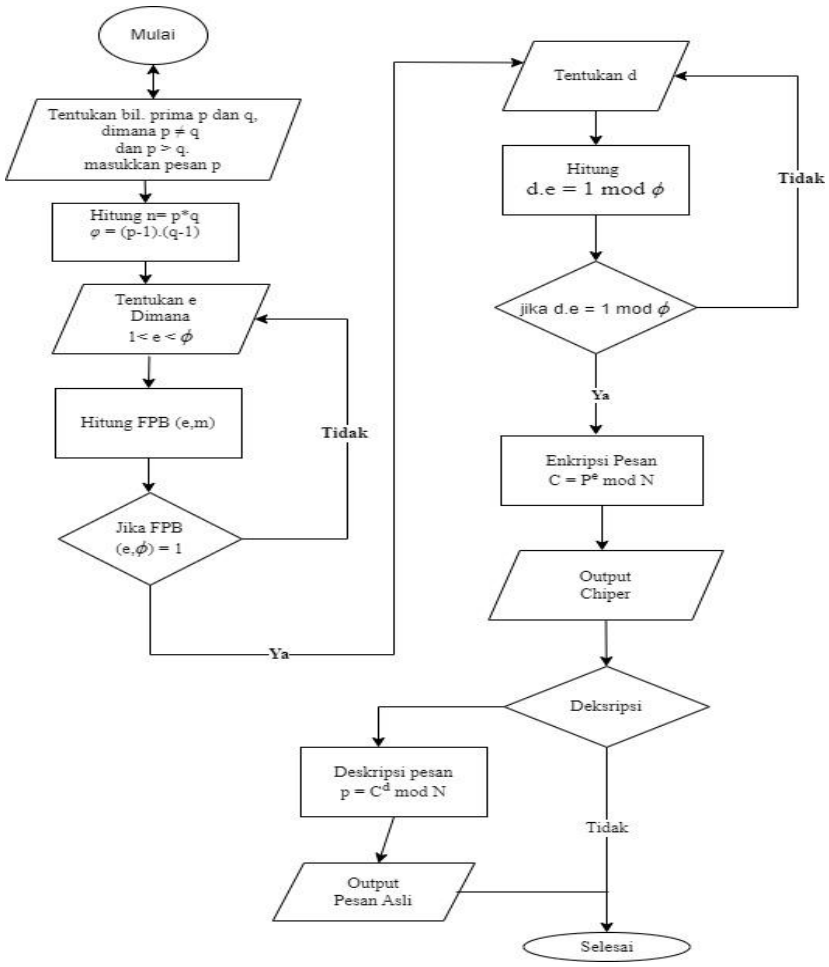
Database adalah kumpulan data yang terorganisir yang disimpan dan diakses secara elektronik dari sistem kompuer. *Database* sangat kompleks bahkan semakin hari semakin dikembangkan. Semakin banyak data pada database maka semakin banyak informasi yang harus diamankan [5].

Algoritma Rivest Shamir Adleman (RSA)

Algoritma RSA merupakan enkripsi yang termasuk jenis asimetris dengan proses enkripsi yang menggunakan sebuah public key dan proses dekripsi yang membutuhkan sebuah private key [6].

Algoritma RSA dijabarkan pada tahun 1997 oleh Ron Rivest, Adi Shamir dan Len Adleman dari *Massachusetts Institute of Technology* (MIT). Huruf RSA itu sendiri juga berasal dari inisial nama mereka (Rivest-Shamir-Adleman).

Clifford Cocks, seorang matematikawan Inggris yang bekerja untuk GCHQ, menjabarkan tentang sistem equivalen pada dokumen internal di tahun 1973. Penemuan Clifford Cocks tidak terungkap hingga tahun 1997 dikarenan alasan top-secret classification. Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di Amerika Serikat sebagai U. S. Patent 4405829. Paten tersebut berlaku hingga 21September 2000. Semenjak Algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi disebagian besar negaranegara lain tidak memungkinkan penggunaan paten. Hal ini menyebabkan hasil temuan Clifford Cocks dikenal secara umum, paten di Amerika Serikat tidak dapat mematenkannya.



Gambar 1. Penerapan Algoritma Rivest Shamir Adleman.

Algoritma kriptografi RSA didesain sesuai fungsinya sehingga menghasilkan kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi pesan. Algoritma RSA disebut menggunakan kunci publik karena kunci enkripsi yang dibuat boleh diketahui semua orang, dan juga bisa melakukan enkripsi pesan tersebut. Sedangkan yang dimaksud kunci privat adalah kunci untuk melakukan dekripsi pesan tidak semua orang boleh mengetahuinya, hanya orang tertentu yang berhak saja untuk melakukan dekripsi pesan. Keamanan algoritma RSA didasarkan pada sulitnya memfaktorkan bilangan besar menjadi factor-faktor primanya. (Yosua Tarigan, et. al.) [7]. Adapun langkah-langkah pembuatan kunci antara lain:

1. Pilih dua buah bilangan prima misal p dan q, adapun p ≠ q dipilih secara acak dan terpisah untuk tiap-tiap p dan q. Hitung nilai N dimana nilai N adalah hasil perkalian antara bilangan p dan q, (N= p.q)
2. Hitunglah nilai Totien Euler dengan rumus $\phi(n)$ = (p-1).(q-1).
   Totien Euler yang dilambangkan sebagai $\phi(n)$ dalam RSA berfungsi memberikan jumlah bilangan bulat positif yang kurang dari *n* dan coprime (relatif prima) dengan *n.*
3. Pilihlah bilangan bulat (*integer*) antara satu dan ϕ, (1 < e < ϕ) yang juga merupakan bilangan koprima dari ϕ.
4. Hitunglah nilai d hingga d.e ≡ 1 (mod ϕ), nilai d berfungsi sebagai eksponen privat yang digunakan untuk mendekripsi pesan yang telah di enkripsi dengan kunci publik.
   adapun untuk mencari d bisa menggunakan rumus = d = $\frac{1+kn}{e}$
   Adapun nilai k adalah hasil percobaan dari nilai 1,2,3, … sehingga menghasilkan nilai d merupakan nilai bulat.
   Adapun kunci publik antara lain:
   a. Nilai bilangan N
   b. Serta bilangan e (digunakan untuk proses enkripsi pesan)

   Adapun kunci privat antara lain:
   a. Nilai bilangan N
   b. Serta bilangan d (digunakan untuk dekripsi pesan)

 https://doi.org/10.56211/helloworld.v3i4.670

Proses Enkripsi dan Dekripsi Pesan

Dalam melakukan proses enkripsi maupun dekripsi pesan algoritma RSA memiliki rumus yang berbeda dalam merubah pesan yang diterimanya. Adapun rumus yang digunakan untuk melakukan enkripsi pesan adalah:

C = *Plaintext*^{e} *Mod* N
Keterangan:
Plaintext : Merupakan text asli yang akan dirubah
e : Merupakan kunci publik yang digunakan untuk enkripsi
N : Merupakan perkalian dua buah bilangan pirma p dan q Sedangkan
untuk merubah chipertext kedalam bentuk semula memerlukan rumus yang berbeda dengan proses enkripsi, rumus dekripsi pesan adalah sebagai berikut:

Plaintext = Chipertext^{d} ***Mod* N**
Keterangan:
Chipertext : Merupakan pesan yang akan dirubah kebentuk asli
d : Merupakan kunci privat yang digunakan untuk dekripsi
N : Merupakan perkalian dua buah bilangan prima p dan q

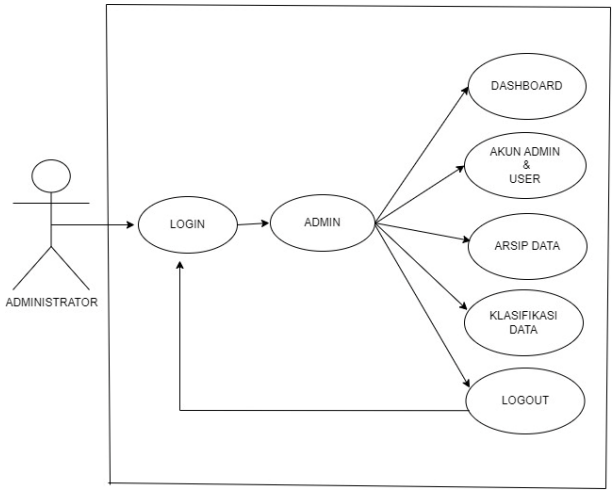
METODOLOGI

Penelitian ini dimulai dengan melakukan metode observasi, dalam metode ini yang dilakukan penulis adalah data-data yang mendukung sistem dengan meneliti cara pengolahan data secara manual di kantor Desa Buntu Bedimbar.

Kemudian melakukan wawancara, yaitu menjelaskan kegiatan ke responden yang terkait topik Penulis secara langsung melakukan sesi tanya jawab ke sekretaris Desa serta beberapa warga Desa Buntu Bedimbar terkait dengan sistem pengarsipan untuk dijadikan panduan dalam pembuatan *website.*

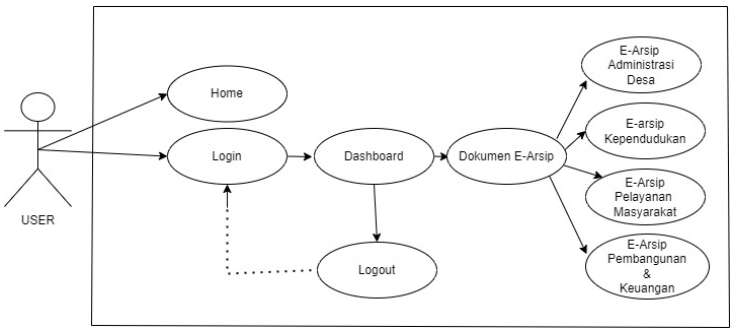
Tahapan selanjutnya ialah dengan melakukan metode studi pustaka Dalam metode ini penulis mengumpilkan data dengan menggunakan Pustaka-pustaka yang telah ada baik itu dari buku maupun jurnal yang berkaitan dengan materi yang dibuat untuk dijadikan referensi

Pemodelan Sistem
Use Case Diagram



Gambar 2. *Use Case Diagram Administrator*

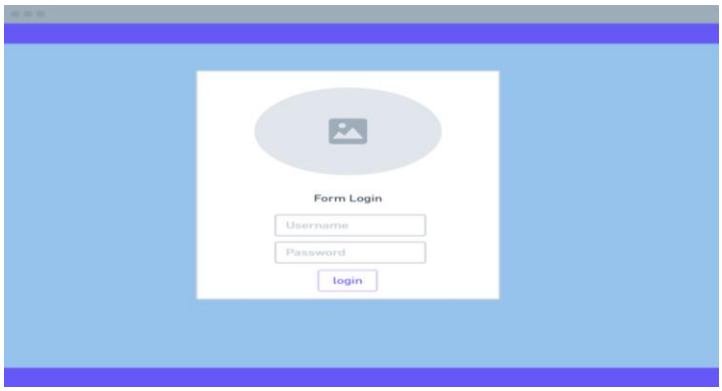
Pada gambar tersebut Menggambarkan *Use Case Diagram* untuk Admin, seorang admin dapat mengakses semua fitur menu aplikasi dari menu data akun admin dan *user*, menu arsip data, dan menu klasifikasi data. Admin juga memiliki wewenang dalam menambah serta melakukan pengeditan dalam data-data yang ada di setiap menu pada aplikasi.



Gambar 3. *Use case Diagram User*

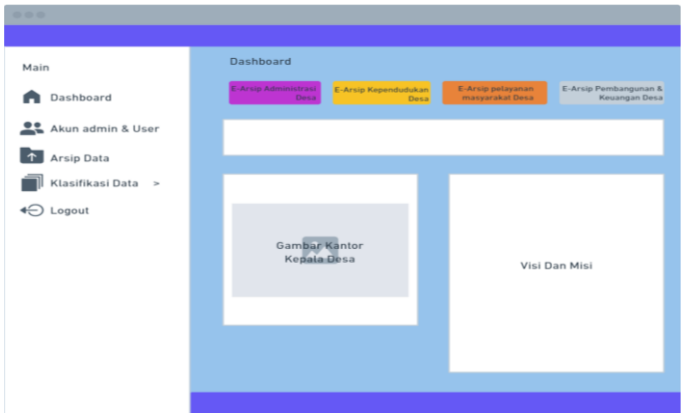
Pada gambar tersebut merupakan *use case diagram* untuk *user*. Seorang *user* dapat melakukan login menggunakan *username* dan *Password,* serta *user* dapat melihat dokumen E-Arsip surat masuk dan keluar seperti E-Arsip Administrasi Desa, E-Arsip Kependudukan, E-Arsip Pelayanan Masyarakat, dan E-Arsip Pembangunan & Keuangan.

Desain Interface



Gambar 4. Tampilan halaman Login

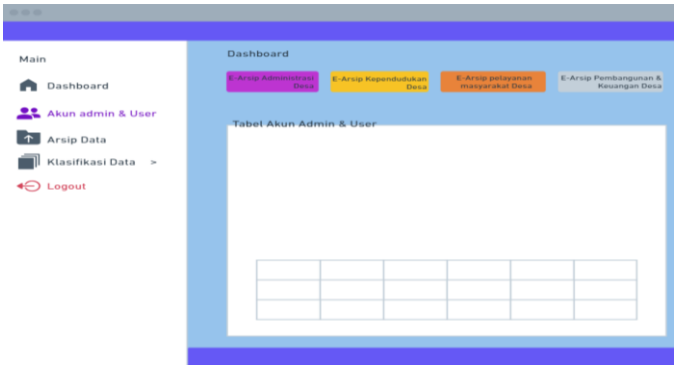
Pada gambar tampilan halaman login yang pertama kali terlihat dan dapat diakses oleh *user*. Pada tampilan ini *user/admin* dapat melakukan login dengan memasukkan username dan password.



Gambar 5. Tampilan Halaman Dashboard Admin

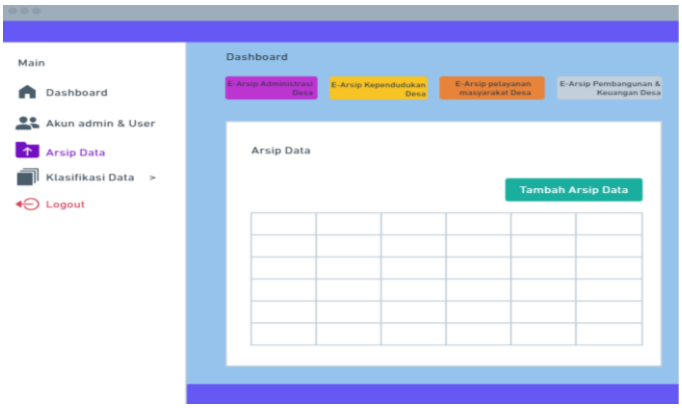
Pada gambar tampilan menu Dashboard ini, admin dapat melihat berapa banyak jumlah setiap Arsip yang diklasifikasikan, serta admin juga dapat melihat visi dan misi pada kantor desa buntu bedimbar.

 https://doi.org/10.56211/helloworld.v3i4.670



Gambar 6. Tampilan akun Admin & User

Pada gambar tampilan ini, admin dapat melihat serta menambah akun admin dan user yang akan mengakses aplikasi E-Arsip nantinya.

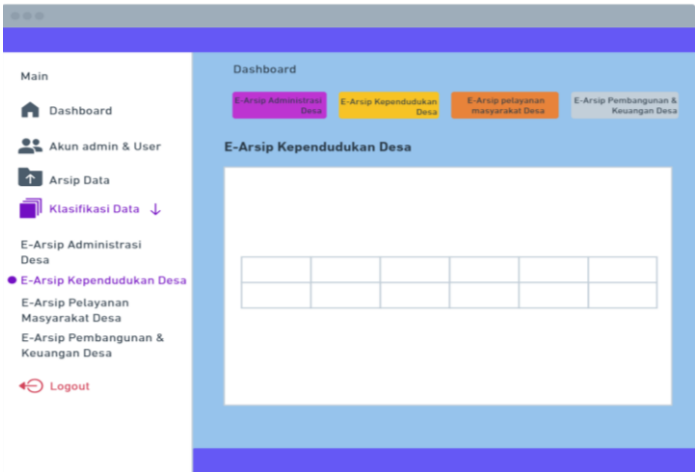


Gambar 7. Tampilan Arsip Data

Pada tampilan ini admin dapat menambahkan serta menghapus data-data arsip yang ada pada kantor desa buntu bedimbar.

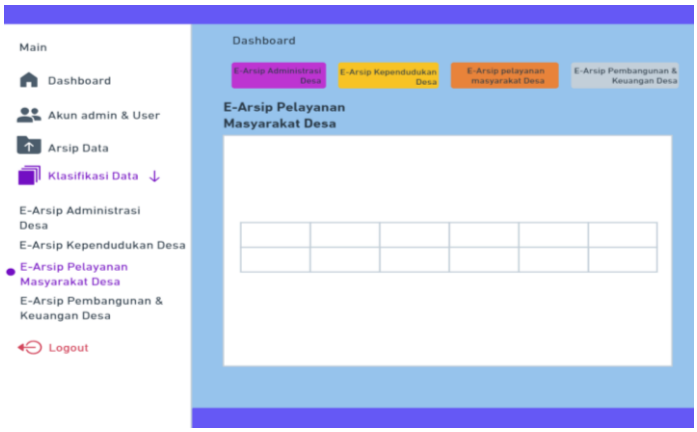
Gambar 8. Tampilan E-Arsip Administrasi Desa.

Pada tampilan ini admin dapat melihat arsip surat sesuai judul dan jenis arsip yaitu jenis arsip Administrasi Desa.



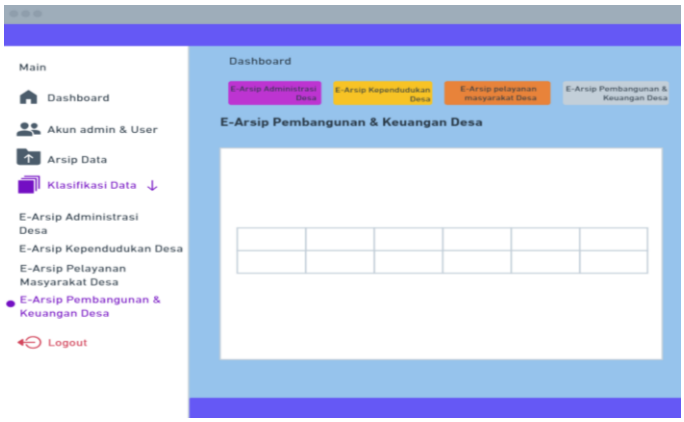
Gambar 9. Tampilan Kependudukan Desa.

Pada tampilan ini admin dapat melihat arsip surat sesuai judul dan jenis arsip yaitu jenis arsip Kependudukan Desa.



Gambar 10. Tampilan E-Arsip Pelayanan Masyarakat Desa.

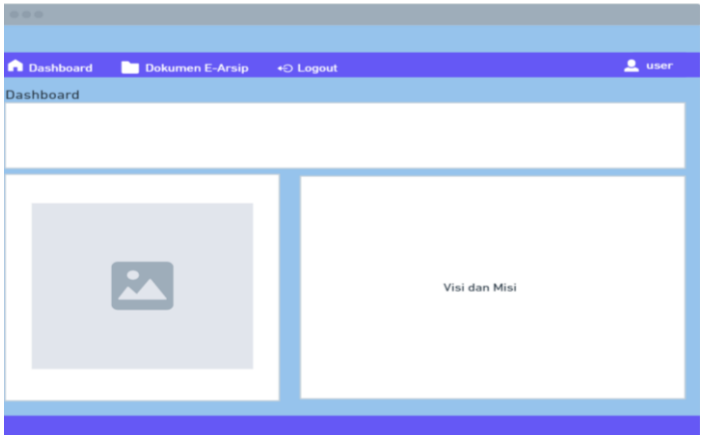
Pada tampilan ini admin dapat melihat arsip surat sesuai judul dan jenis arsip yaitu jenis Arsip Pelayanan Masyarakat Desa.



Gambar 11. Tampilan E-Arsip Pembangunan & Keuangan Desa.

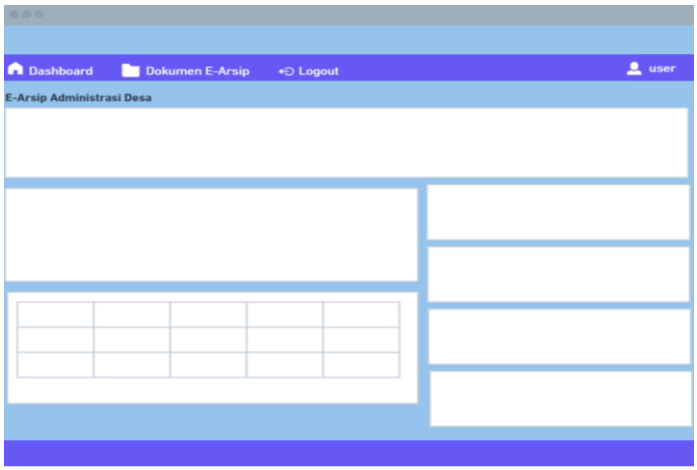
Pada tampilan ini admin dapat melihat arsip surat sesuai judul dan jenis arsip yaitu jenis arsip Pembangunan & Keuangan Desa.

 https://doi.org/10.56211/helloworld.v3i4.670



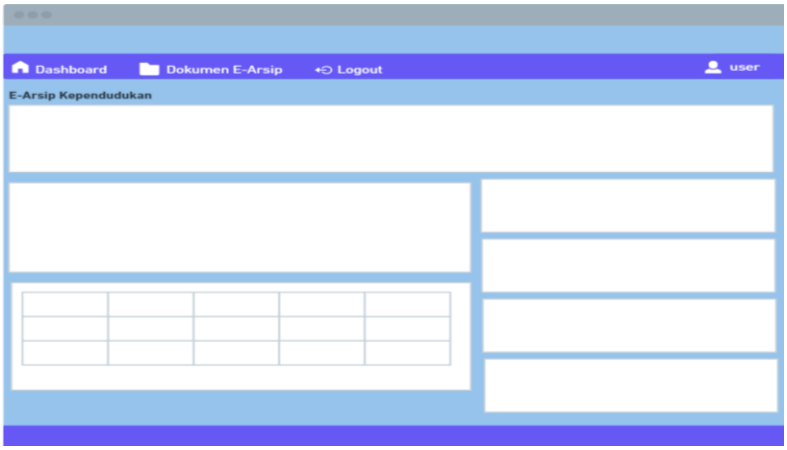
Gambar 12. Tampilan Dashboard user.

Pada tampilan ini User dapat melihat visi dan misi serta fitur Dokumen Arsip dan fitur Logout pada Aplikasi.



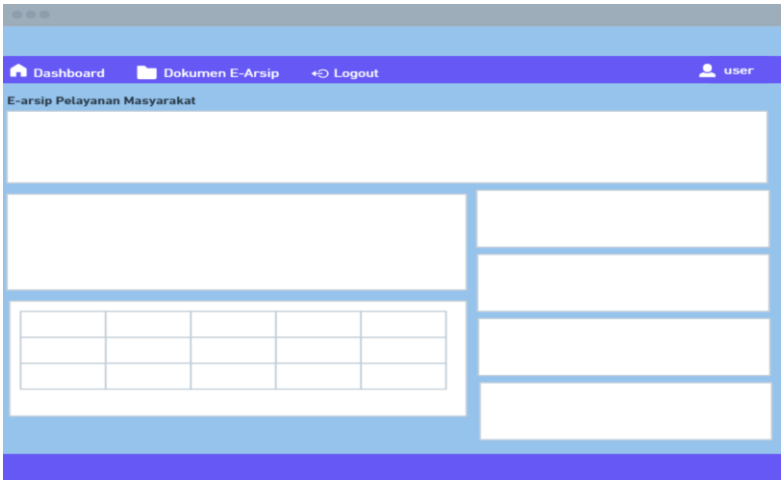
Gambar 13. Tampilan E-Arsip Administrasi Desa Pada User.

Pada tampilan ini user dapat melihat dokumen arsip administrasi desa yang sudah di input oleh admin pada aplikasi E-Arsip.



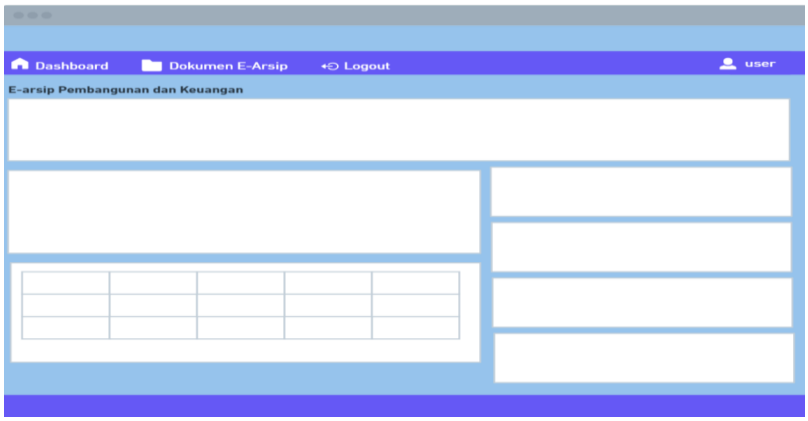
Gambar 13. tampilan E-Arsip Kependudukan Pada User.

Pada tampilan ini user dapat melihat dokumen arsip kependudukan yang sudah di input oleh admin pada aplikasi E-Arsip.



Gambar 14. tampilan E-arsip Pelayanan Masyarakat Pada User.

Pada tampilan ini user dapat melihat dokumen arsip Pelayanan Masyarakat yang sudah di input oleh admin pada aplikasi E-Arsip.



Gambar 15. Tampilan E-Arsip Pembangunan dan Keuangan Pada User.

Pada tampilan ini user dapat melihat dokumen arsip Pembangunan dan Keuangan yang sudah di input oleh admin pada aplikasi E-Arsip.

HASIL DAN PEMBAHASAN

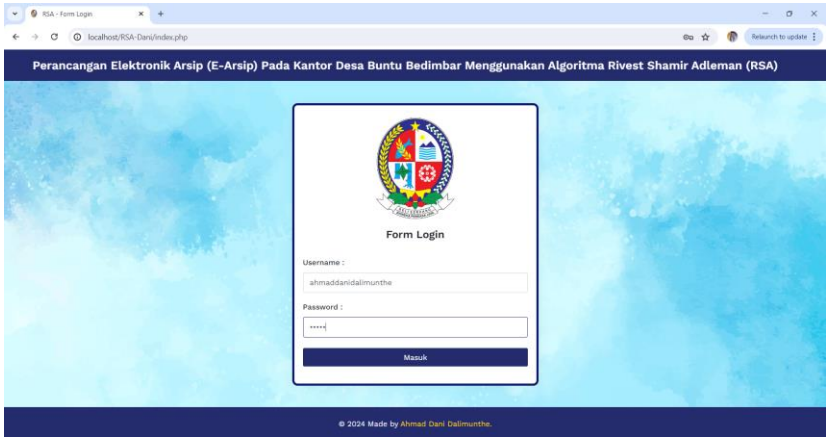
Implementasi

Aplikasi ini merupakan sistem pengamanan data pada Arsip surat masuk dan surat keluar yang bertujuan untuk menjaga keamanan data-data dan untuk mempermudah pegawai dalam membantu pekerjaannya dalam melakukan pelayanan kepada masyarakat.

Tampilan Login Pengguna

Pada halaman login pengguna, admin atau user akan memasukkan username dan password dengan benar untuk bisa mengakses login kedalam aplikasi.

 https://doi.org/10.56211/helloworld.v3i4.670



Gambar 16. Tampilan Login Pengguna

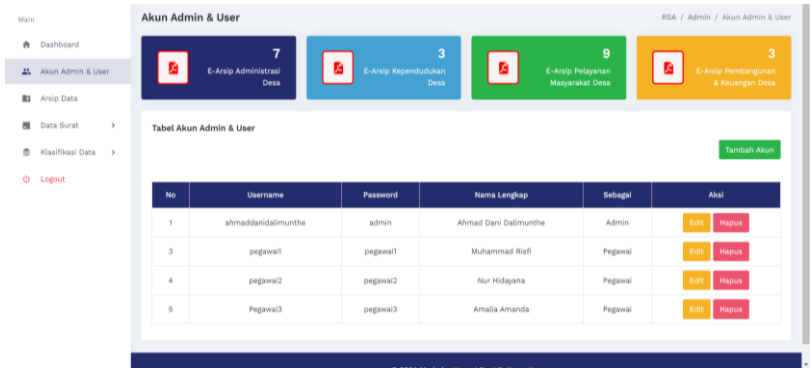
Tampilan Halaman Dashboard Admin

Gambar 17. Tampilan Halaman Dashboard Admin

Tampilan Halaman Dahsboard User

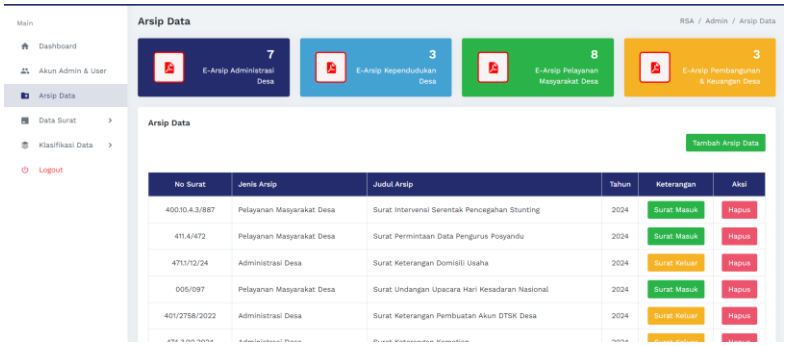
Gambar 18. Tampilan Halaman Dashboard User

Tampilan Akun Admin & User



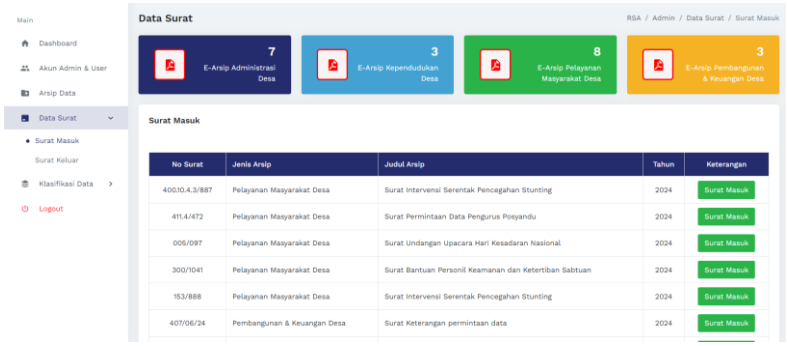
Gambar 19. Tampilan Akun Admin & User

Tampilan Arsip Data



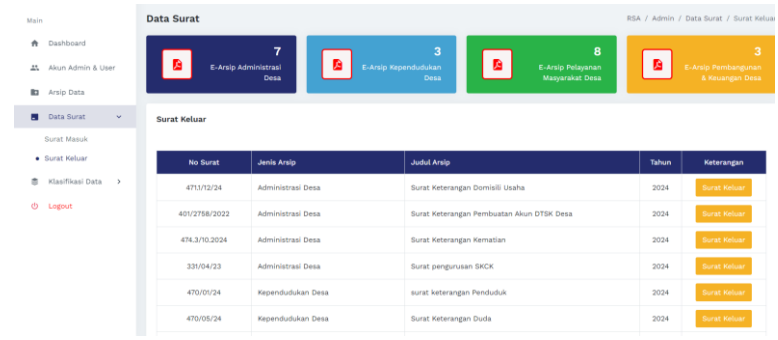
Gambar 20. Tampilan Arsip Data

Tampilan Data Surat Masuk



Gambar 21. Tampilan Data Surat Masuk

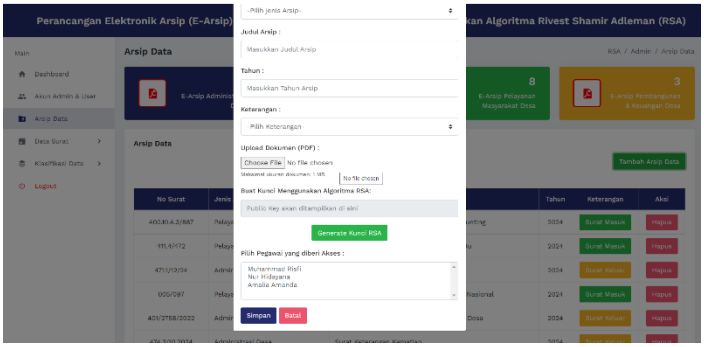
Tampilan Data Surat Keluar



Gambar 22. Tampilan Data Surat Keluar

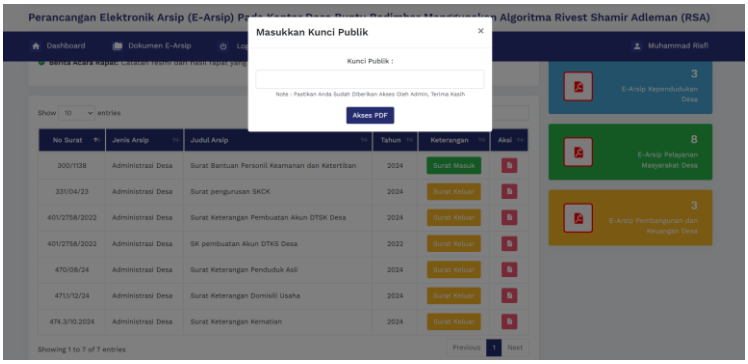
 https://doi.org/10.56211/helloworld.v3i4.670

Tampilan Generate Kunci Algoritma RSA pada Fitur Tambah Data



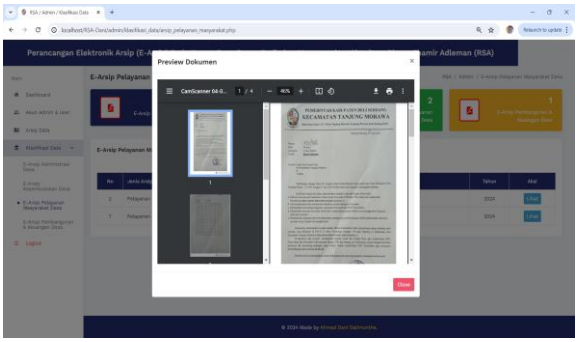
Gambar 23. Tampilan Generate Kunci Algoritma RSA pada Fitur Tambah Data

Tampilan Memasukkan Kunci Publik Data Surat pada Akun User



Gambar 24. Tampilan Memasukkan Kunci Publik Data Surat pada Akun User

Tampilan Hasil Data Surat Setelah Berhasil Memasukkan Kunci



Gambar 25. Tampilan Hasil Data Surat Setelah Berhasil Memasukkan Kunci

KESIMPULAN DAN SARAN

Berdasarkan implementasi yang telah dilakukan pada pembahasan sebelumnya, maka dapat diambil kesimpulan sebagai berikut: Penelitian ini menghasilkan sebuah aplikasi Pengamanan E-Arsip surat menyurat pada kantor desa buntu bedimbar. Aplikasi ini dibuat untuk membantu pegawai dalam membantu tugas tentang surat menyurat yang sebelumnya masih dilakukan dengan cara manual. Aplikasi Elektronik Arsip (E-Arsip) ini dibangun menggunakan perancangan model UML (Unifield Modelling Language) perancangan dan pengembangan pada aplikasi E-Arsip ini menggunakan beberapa bahasa pemrograman yaitu HTML, PHP, CSS, dan JavaScript. Penerapan algoritma Rivest Shamir Adleman pada aplikasi ini sangat membantu dalam mengenkripsi data dengan kecepatan yang sangat efisien. Dengan menggunakan Enkripsi Publik key dan Private Key file-file tersebut semakin kuat dan aman dari pencurian data.

Saran

Dalam aplikasi yang telah dibangun disadari masih terdapat banyak kekurangan, oleh karena itu untuk pengembangan selanjutnya disarankan:
1. Sistem yang telah dibuat ini masih terbatas pada pengarsipan data. Untuk pengembangan selanjutnya diharapkan untuk menambahkan fitur tanda tangan digital dengan menggunakan QR Code.
2. Penulis juga menyarankan untuk peneliti berikutnya dapat menggunakan algoritma yang bisa melakukan QR Code pada aplikasi ini, untuk memudahkan pegawai dalam melakukan enkripsi data yang lebih simple dan modern.

DAFTAR PUSTAKA

[1] Fathurrahman. 2018. "Pentingnya Arsip Sebagai Sumber Informasi". Jurnal Ilmu Perpustakaan dan Informasi. Vol 3 No 2.

[2] Shella Ayurindah. 2022. "PERAN TATA USAHA SEKOLAH DALAM PENGELOLAAN ARSIP SEKOLAH". Jurnal Manajemen Pendidikan Islam. Vol 1 No 1.

[3] Yudin W,Dhian Nur Rahayu. 2010. "ANALISIS METODE PENGEMBANGAN SISTEM INFORMASI BERBASIS WEBSITE : A LITERATUR REVIEW". Jurnal Publikasi Ilmiah bidang Teknologi Informasi dan Komunikasi. ISSN : 1907-8420.

[4] A.Nurkholis. 2022. "Implementasi Sistem Informasi Profil Sekolah Berbasis Web pada SMK Minhadlul Ulum" *Jurnal Teknologi dan Sistem Informasi*. Vol 4 No 1.

[5] Tomy Satria Alasi dan Ahmad Taufik. 2020. "Algoritma Vigenere Chiper Untuk Penyandian Record Informasi Pada Database". *Jurnal Informasi Komputer Logika*. Vol 1 No 4.

[6] Ade Rahayu,Amanda,DKK. 2024. "Perbandingan *Algoritma RSA* dengan *Algoritma Blowfish* Pada Perancangan Aplikasi Keamanan Data". Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI). Vol 7 No 1.

[7] Yosua Tarigan, et. al. "Aplikasi Smart School Dengan Pengamanan Data Menggunakan Metode RSA (Rivest Shamir Adleman) Pada PKBM Hanuba Medan". *Jurnal Cybertech*, vol 04. No 2, Februari 2021, https://ojs.trigunadharma.ac.id/.

[8] Achmad Fikri dan Indra. "Perancangan Sistem Informasi Jadwal Dokter Menggunakan Framework Codeigner". *Jurnal Media Infotama.* Vol 16 No 1.

[9] Alfarissi, Kanda, Redo, DKK . "Algoritma RSA Kombinasi dan Skema QR Code untuk Mengamankan Data Penjualan Tiket Online". ISBN : 979-587-705-4. Vol 3 No 1.

[10] Ertie Nur Hartiwati. 2022. "APLIKASI INVENTORI BARANG MENGGUNAKAN JAVA DENGAN PHPMYADMIN" ISSN: 2615-3165 Vol 5 No 1.

[11] Hasan, S. & Muhammad, N. 2020. "SISTEM INFORMASI PEMBAYARAN BIAYA STUDI BERBASIS WEB PADA POLITEKNIK SAINS DAN TEKNOLOGI WIRATAMA MALUKU UTARA". *Indonesian Journal on Information System*. Vol 5 No 1.

[12] Husni Thamrin. 2021. "PELATIHAN PEMROGRAMAN CSS DAN HTML DI SMK AVICENA". *Jurnal Pengabdian dan Pemerdayaan Masyarakat*. Vol 4 No 1.

[13] Ira Murni,Atika,DKK. 2023. "Pengamanan Pesan Rahasia dengan Algoritma Vignere Chiper Menggunakan PHP". *Journal on Education*. Vol 05 No 02.

[14] Romney, Marshall B. & Paul John Steinbart. 2015. "Pengertian Sistem Menurut Marshall B Romney Dan Paul John Steinbart". *Sistem Informasi Akuntansi*.

[15] Rivest, R. L., Shamir, A., & Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. Vol. 21(2): 120-126.

 https://doi.org/10.56211/helloworld.v3i4.670