COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

IMPLEMENTASI METODE RSA DALAM PEMILIHAN UMUM BERBASIS WEB

Zaid Abdurahman[1], Sabrina Aulia Rahmah[2*], Andy Satria[3]

1,2,3) Prodi Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa, Indonesia

*Coresponding Email: **zaidabdurahman3@gmail.com**

Abstrak

Pemilihan umum berbasis web menjadi solusi efektif untuk mengurangi risiko kecurangan dalam pemilu, terutama dalam proses perhitungan suara yang sering kali rawan manipulasi, seperti pencoblosan sebelum pemilihan, pemilih ganda, kesalahan penghitungan manual, serta proses penghitungan yang lama dan tidak real-time. Dalam penelitian ini, algoritma RSA digunakan untuk meningkatkan keamanan pemilihan melalui enkripsi suara pemilih. Sistem dikembangkan menggunakan PHP dan MySQL, dengan keamanan login yang hanya mengizinkan pemilih memberikan suara satu kali. Hasil penelitian menunjukkan bahwa implementasi metode RSA berhasil meningkatkan keamanan dan efisiensi proses pemilihan, sehingga sistem ini berpotensi menjadi model pemilihan berbasis web yang lebih luas

Kata Kunci: Algoritma RSA, Pemilihan Umum , Enkripsi, E-Voting

Abstract

Web-based elections are an effective solution to reduce the risk of fraud in elections, particularly in the vote counting process, which is often vulnerable to manipulation, such as early voting, double voting, manual counting errors, and the lengthy and non-real-time counting process. In this study, the RSA algorithm is used to enhance election security through the encryption of voters' ballots. The system is developed using PHP and MySQL, with secure login credentials that allow each voter to cast their vote only once. The results show that the implementation of the RSA method successfully improves the security and efficiency of the election process, making this system a potential model for broader web-based elections.

Keywords: : RSA Algorithm, Election, Encryption, E-Voting

PENDAHULUAN

Sistem E-Voting (pemungutan suara elektronik) dapat didefinisikan sebagai model dan konsep pemungutan suara baru. E-Voting telah menjadi salah satu teknologi yang signifikan di seluruh dunia menggantikan pemungutan suara konvensional. Perkembangan teknologi

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

komunikasi dapat membuat mereka yang lokasi nya jauh secara geografis dapat mengakses evoting menjadi lebih nyaman dan mudah diakses saat pemungutan suara elektronik.

Di era teknologi informasi yang modern, penggunaan sistem E-Voting semakin banyak ditemui dalam proses pemilu. Saat ini banyak aspek penting yang membut evoting sangat penting mulai dari meringankan kerja panitia agar tidak terjadi kelehahan yang bisa berujung kematian mulai dari menjaga tps dan saat melakukan penghitungan suara secara manual. Namun saat ini keamanan menjadi perhatian utama karena adanya risiko ancaman terhadap legitimasi pemungutan suara online. banyak negara yang mengalami insiden keamanan terkait sistem E-Voting, seperti manipulasi suara dan pencurian data pemilih, kepercayaan masyarakat terhadap integritas dan validitas sistem e-voting sangat penting bagi negara mereka. implementasi yang sukses. Banyak pemilih bahkan peserta sendiri yang meragukan keamanan dan kemampuan sistem E-Voting dalam mencegah manipulasi. Meningkatkan kepercayaan ini merupakan langkah penting agar sistem E-Voting dapat diterima secara luas.

Dalam penelitian ini, metode algoritma RSA (Rivest-Shamir-Adleman) diusulkan sebagai solusi untuk meningkatkan keamanan sistem e-voting. RSA adalah salah satu algoritma kriptografi asimetris yang umum digunakan untuk melindungi data melalui enkripsi dan dekripsi menggunakan kunci publik dan privat. Algoritma ini diimplementasikan dalam sistem pemilihan berbasis web. Sistem ini dikembangkan dengan menggunakan bahasa pemrograman PHP dan basis data MySQL, serta dilengkapi dengan mekanisme login yang memastikan hanya pemilih yang sah dapat memberikan suara satu kali.

KAJIAN TEORI

Pada bab kali ini akan di bahas berbagai teori dan konsep yang mendasari tentang Implementasi metode RSA dalam pemilihan umum. Tinjaun pustaka berfungsi sebagai pedoman dan memberikan konsep dan pemahaman yang kuat serta tidak keluar dari masalah atau penelitian Implementasi metode RSA dalam pemilihan umum.

A. E-Voting

E-Voting atau pemilihan secara elektronik merupakan sistem yang memungkinkan

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

pemilih untuk mencatat pilihannya yang bersifat rahasia secara elektronik yang teramankan. Pengertian lainnya adalah sebuah proses yang dibuat untuk membuat surat suara, memberikan, menghitung, menayangkan perolehan suara, serta menghasilkan dan memelihara jejak audit secara digital (Yuda Pratama Putra, 2021),

B. Kriptografi RSA

RSA adalah salah satu algoritma block cipher, atau bekerja per blok data, yang menggabungkan teks biasa menjadi blok-blok terlebih dahulu sebelum dienkripsi hingga menjadi teks cipher (Haryanto, 2021). Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor-faktor prima dari bilangan yang besar, yang dalam hal ini adalah memfaktorkan n menjadi a dan b. Kemudian sekali n berhasil difaktorkan menjadi a dan b, maka $m = (a - 1)(b - 1)$ dapat dihitung. Selanjutnya karena kunci enkripsi diutamakan e bebas (tidak rahasia),
maka kunci dekripsi d dapat dihitung dari persamaan $e.d = 1 \ (mod\ m)$. Hal tersebut merupakan proses dekripsi yang dilakukan oleh orang yang tidak berhak.

C. Enkripsi & Deskripsi

RSA Berikut langkah-langkah proses enkripsi dan dekripsi pada algoritma RSA :

i. Ambil kunci publik yang telah dibangkitkan pada proses sebelumnya yaitu (e,n).
ii. Untuk proses enkripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.8. $ci = mi\ emod n$ (2.8)
iii. Ambil kunci privat yang telah dibangkitkan pada proses sebelumnya yaitu (d,n).
iv. Untuk proses dekripsi menggunakan rumus yang ditunjukkan pada Persamaan 2.9.
$mi = ci\ dmod\ n$ (2.9)
dimana :
c = chipertext
m = Plaintext

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

D. PHP

bahasa pelengkap HTML yang memungkinkan pembuatan aplikasi dinamis dengan pengolahan dan pemrosesan data. Sintaks yang diberikan dijalankan sepenuhnya pada server, dan hanya hasilnya yang dikirimkan ke browser. PHP merupakan bahasa skrip yang ditempatkan di server dan diproses di sana. Hasilnya kemudian dikirimkan ke client, di mana pengguna menggunakan browser. PHP dikenal sebagai bahasa scripting yang menyatu dengan tag HTML, dieksekusi di server, dan digunakan untuk membuat halaman web dinamis, mirip dengan *Active Server Pages* (ASP) atau *Java Server Pages* (JSP). PHP adalah perangkat lunak Open Source.(Hermiati Reza et al., 2020).

E. MySQL

program database server yang mampu menerima dan mengirimkan datanya dengan sangat cepat, multi user, serta menggunakan perintah standar SQL (*Structured Query Language*).(Ahmadar et al., 2021)

MySQL merupakan RDBMS (*Relational Database Management System*) server. RDBMS adalah program yang memungkinkan pengguna databaseuntuk membuat, mengelola, dan menggunakan data pada suatu model relational. Dengan demikian, tabel-tabel yang ada pada databasememiliki relasi antara satu tabel dengan tabel lainnya.

METODE PENELITIAN

Penerapan kriptografi dianggap sebagai solusi untuk meningkatkan keamanan, namun implementasinya penuh dengan tantangan, dampak negatif perkembangan teknologi terhadap keamanan E-Voting menjadi sorotan, sementara perlindungan data dalam E-Voting masih memadai. Metode yang digunakan dalam penelitian ini mencakup beberapa tahapan penting, yaitu pengumpulan data, analisis, pemodelan, dan pengujian model. Berikut adalah tahapan-tahapan yang dilakukan dalam penelitian ini.

1. Pengumpulan Data

Pengumpulan data d alam penelitian ini sangat di perlukan untuk

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

mendapatkan ide atau informasi yang akurat berikut adalah metode pengumpulan data.

a. Peneliti melakukan sejumlah pengamatan atau observasi dari pemungutan suara konvensional dan membandingkan dengan peumungutan suara elecktronik.
b. peneliti melakukan studi literatur pada jurnal dan buku yang berkaitan dengan *E-voting* yang digunakan sebagai refrensi membuat penelitian ini.

2. Studi Kasus

Studi kasus bertujuan untuk melakukan implementasi nyata keamanan E-voting dengan algoritma RSA.

A. Pembuatan kunci Private keys dan Public keys

Pembuatan kunci Private keys dan Public keys menggunakan Openssl, public keys digunakan untuk proses enkripsi database ,sedangkan private keys untuk deskripsi database

Buat kunci

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

Ekstrak kunci

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

B. Registrasi pemilih

Registrasi pemilih dilakukan dengan cara mendaftarkan email kita kepada Panitia dan nanti akan dikirim id dan password nya melalui email terkait.

C. Proses pemilihan

-Pemilih akan membaca visi dan misi setiap kandidat

-Pemilih memilih kandidat yang di inginkan

D. Peneriman suara

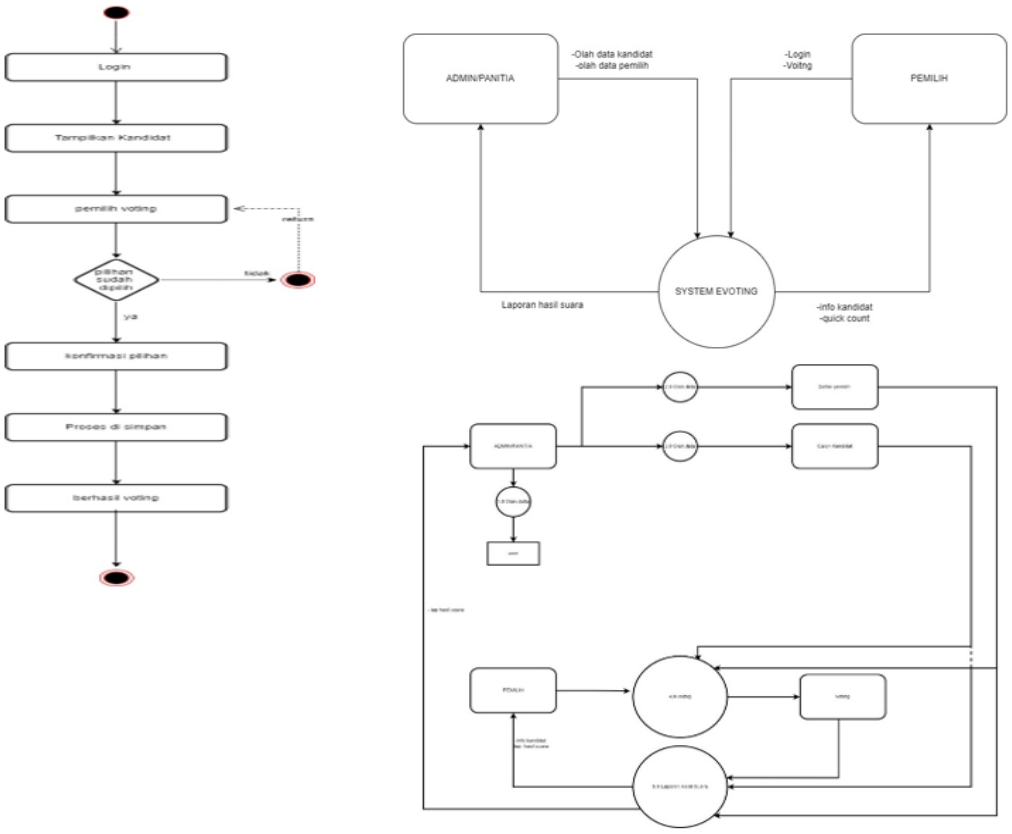
Suara pemilih akan dikumpulkan dan dihitung oleh sistem tetapi hasil perolehan suara akan di umum setelah selesai pemilihan.

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

3. Rancangan Perangkat Lunak

Rancangan penelitian yang bertujuan untuk pedoman dalam melaksanakan proses penelitian. Desain penelitian bertujuan sebagai pegangan yang jelas dan terstruktur kepada peneliti dalam melakukan penelitiannya.

Beikut adalah beberapa rancangan perangkat lunak



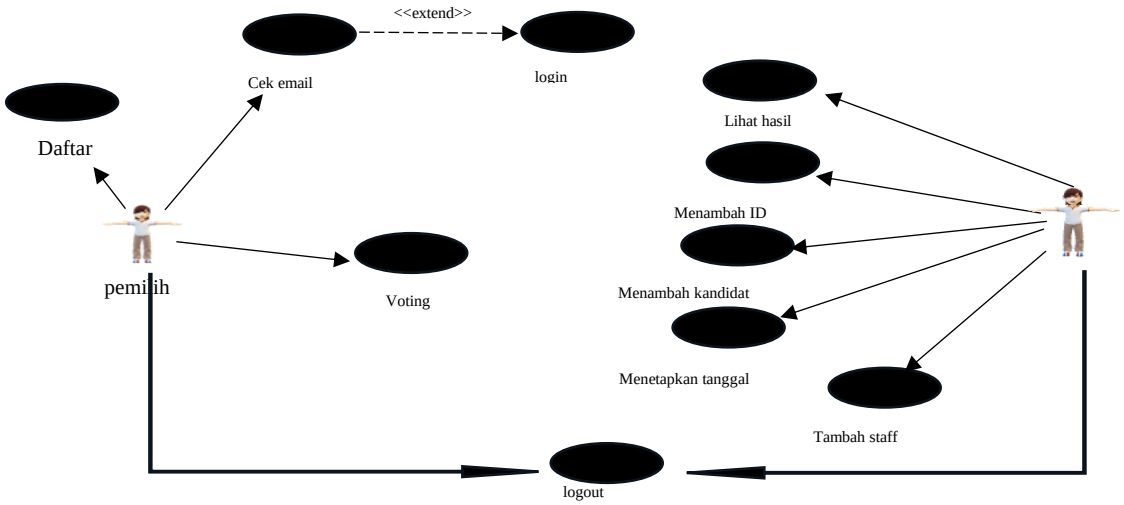
Gambar 1 Beberapa Diagram yang di perlukan untuk merancang aplikasi

4. Desain Sistem

Berdasarkan hasil analisis sistem, dihasilkan keluaran skenario yang ditampilkan dalam format diagram UML. Dalam penelitian ini UML digunakan sebagai desain pemodelan sistem karena bahasa pemrograman yang digunakan dalam pengembangan sistem mendukung implementasi dan konfigurasi bahasa yang

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

berpusat pada objek. Diagram yang digunakan untuk memodelkan sistem adalah *diagram use case*, *class diagram*, dan *diagram actify*.



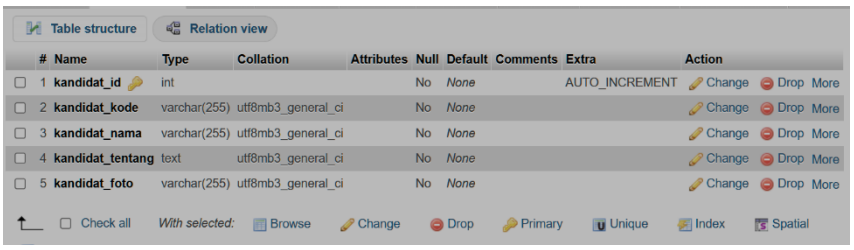
Gambar 2 Use case Diagram pada Voting

HASIL DAN PEMBAHASAN

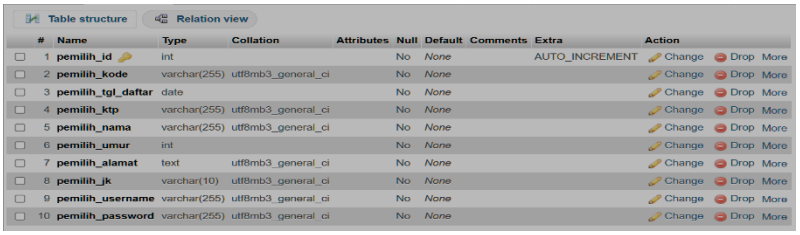
1. Implementasi sistem

   dengan membuat database dengan Mysql dengan nama E_Voting dan membuat 4 tabel yang berupa tabel kandidat, tabel pemilih, tabel user, tabel voting.

   Berikut adalah stuktur table yang di buat

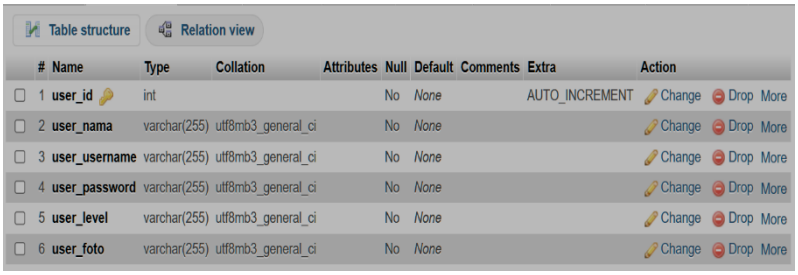


Gambar 3 Stuktur Kandidat



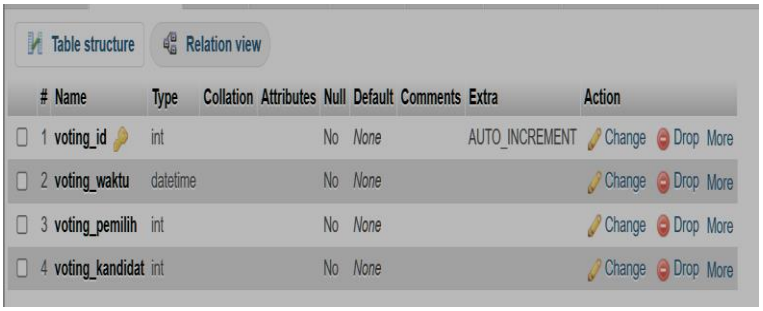
COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

Gambar 4 Stuktur Pemilih



#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	user_id	int			No	None		AUTO_INCREMENT	Change Drop More
2	user_nama	varchar(255)	utf8mb3_general_ci		No	None			Change Drop More
3	user_username	varchar(255)	utf8mb3_general_ci		No	None			Change Drop More
4	user_password	varchar(255)	utf8mb3_general_ci		No	None			Change Drop More
5	user_level	varchar(255)	utf8mb3_general_ci		No	None			Change Drop More
6	user_foto	varchar(255)	utf8mb3_general_ci		No	None			Change Drop More

Gambar 5 Stuktur User



#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	voting_id	int			No	None		AUTO_INCREMENT	Change Drop More
2	voting_waktu	datetime			No	None			Change Drop More
3	voting_pemilih	int			No	None			Change Drop More
4	voting_kandidat	int			No	None			Change Drop More

Gambar 6 Stuktur Voting

2. Template HTML

   Pembuatan template Html yang menjadi tampilan pada halaman projek dalam Folder template, penulis membuat beberapa template yang di perlukan seperti :

   a. Halaman Login.

   b. Halaman Admin.

   c. Halaman utama.

   d. Halaman voting.

   e. Halaman quick count.

   f. Halaman panitia.

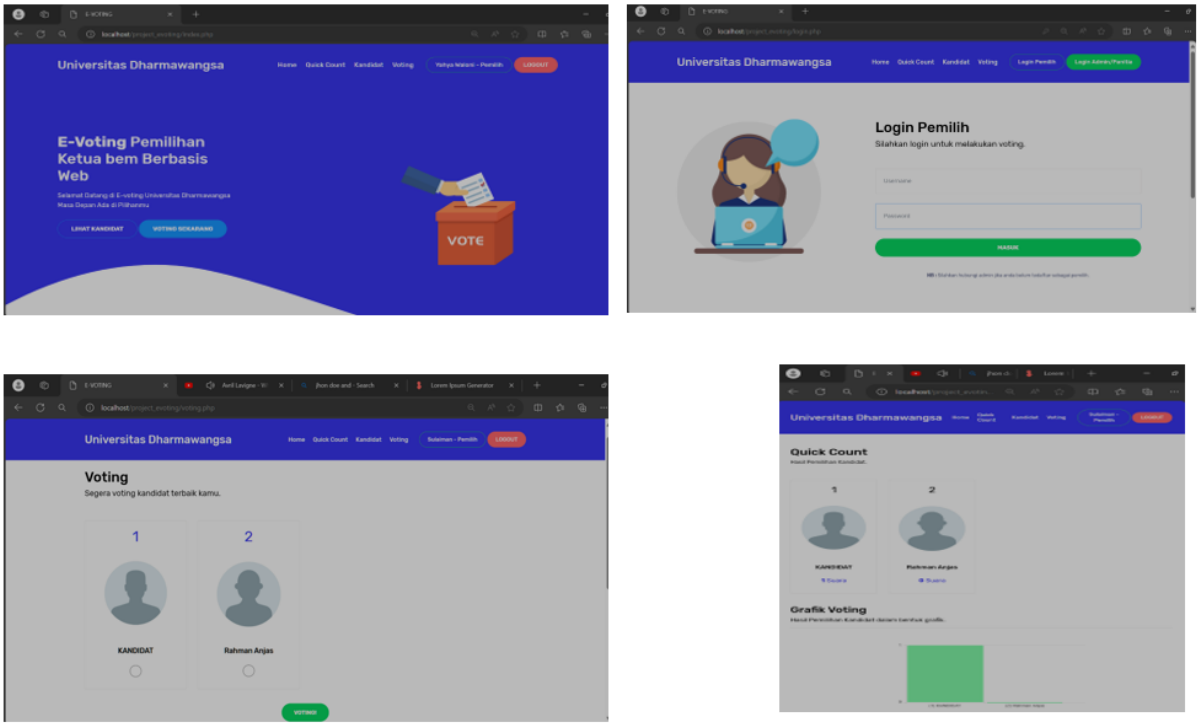
   h. Halaman koneksi untuk mengkoneksikan web dengan database.

   Semua halaman tersebut di tulis dengan format HTML dengan Bahasa pemprograman javascript dan PHP.

3. Hasil Tampilan Aplikasi

   Setelah membuat database dan template HTML kita mendapatkan tampilan aplikasi seperti gambar berikut

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech



Gambar 7 Tampilan aplikasi

4. Pengujian

Pada pengujian peneliti menggunakan tidak menguji secara manual karena akan memakan waktu yang lama , Peneliti menggunakan aplikasi selenium webdriver untuk menguji antar muka web yang akan di gunakan, peneliti menggunkan selenium dikarenakan selenium di sudah teintegrasi dalam banyak bahasa pemprograman dan selenium bisa digunakan dalam antar lintas platform.

Pada tabel 1 dan 2 peneliti sudah membuat tabel black box sebagai tabel pengujian dan membuat beberapa skenario uji, berikut adalah isi dari tabel 1 dan 2

Tabel 1 Pengujian Voting

Skenario Uji	Langkah-langkah Uji	Input	Hasil yang Diharapkan
Pengguna Memilih Kandidat	1. Buka halaman utama aplikasi	-	Halaman utama aplikasi muncul dengan benar

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

	2. Login sebagai pemilih dengan kredensial valid	Username: pemilih1	Halaman berpindah ke halaman pemilihan kandidat
	3. Pilih kandidat tertentu untuk pemilihan	Password: pemilih1	Pesan sukses muncul: "Berhasil memilih kandidat"
	4. Verifikasi pemilihan telah direkam dengan benar	Pilih kandidat	Data pemilihan kandidat tercatat dalam sistem dengan benar
	5. Keluar dari akun pemilih		Logout berhasil, kembali ke halaman login
Admin Mengelola Data Kandidat	1. Buka halaman admin aplikasi	-	Halaman admin aplikasi muncul dengan benar
	2. Login sebagai admin dengan kredensial valid	Username: admin1	Halaman berpindah ke halaman manajemen kandidat
	3. Tambahkan kandidat baru ke dalam daftar	Password: admin1	Kandidat baru berhasil ditambahkan, muncul pesan sukses
	4. Edit informasi kandidat yang sudah ada		Informasi kandidat terbaru tersimpan dengan benar
	5. Hapus kandidat dari daftar		Kandidat yang dihapus tidak muncul dalam daftar
	6. Verifikasi perubahan berhasil terjadi		Perubahan (tambah, edit, hapus) kandidat tercatat dalam sistem dengan benar
	7. Keluar dari akun admin		Logout berhasil, kembali ke halaman login

Tabel 2 Pengujian Login

Skenario Uji	Langkah-langkah Uji	Input	Hasil yang Diharapkan
Login dengan kredensial valid	1. Buka halaman login aplikasi e-voting	-	Halaman login muncul dengan benar
	2. Masukkan username yang valid	Username: pemilih1	Field username terisi dengan benar
	3. Masukkan password yang valid	Password: pemilih1	Field password terisi dengan benar
	4. Klik tombol Login		Halaman berpindah ke halaman dashboard atau halaman selanjutnya sesuai hak akses pemilih
	5. Verifikasi login berhasil		Pesan selamat datang atau tampilan halaman dashboard pemilih muncul
	6. Keluar dari akun		Logout berhasil, kembali ke halaman login atau halaman utama jika belum login sebelumnya
Login dengan kredensial tidak valid	1. Buka halaman login aplikasi e-voting	-	Halaman login muncul dengan benar

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

	2. Masukkan username yang tidak valid	Username: username_tidak_valid	Field username terisi dengan data yang tidak valid
	3. Masukkan password yang tidak valid	Password: password_tidak_valid	Field password terisi dengan data yang tidak valid
	4. Klik tombol Login		Tidak ada perpindahan halaman atau tetap di halaman login dengan pesan error atau peringatan bahwa kredensial tidak valid
	5. Verifikasi pesan error muncul		Pesan error "Username atau Password Salah" atau pesan yang sesuai dengan implementasi aplikasi
Login tanpa mengisi semua field	1. Buka halaman login aplikasi e-voting	-	Halaman login muncul dengan benar
	2. Biarkan field username kosong	Username: "	Field username tidak terisi
	3. Biarkan field password kosong	Password: "	Field password tidak terisi
	4. Klik tombol Login		Tidak ada perpindahan halaman atau tetap di halaman login dengan pesan error atau peringatan untuk mengisi semua field
	5. Verifikasi pesan error muncul		Pesan error "Username dan Password harus diisi" atau pesan yang sesuai dengan implementasi aplikasi

SIMPULAN

Berdasarkan penelitian yang telah dilakukan, sistem e-voting yang menerapkan kriptografi RSA terbukti mampu memberikan lapisan keamanan yang efektif dalam melindungi data pemilih serta hasil pemilihan. Kriptografi RSA bekerja dengan menggunakan pasangan kunci publik dan kunci pribadi, yang memungkinkan proses enkripsi dan dekripsi data dilakukan dengan aman. Dengan mekanisme ini, akses tidak sah terhadap informasi pemilih dapat dicegah, sehingga risiko manipulasi data maupun kebocoran informasi menjadi lebih kecil. Hal ini menjadikan sistem e-voting lebih andal dan mampu menjaga kerahasiaan serta integritas data selama proses pemilihan berlangsung.

Selain itu, penerapan kriptografi RSA dalam sistem e-voting diharapkan dapat meningkatkan kepercayaan masyarakat terhadap metode pemilihan elektronik. Keamanan yang lebih terjamin akan mengurangi kekhawatiran dan skeptisisme terkait potensi kecurangan atau

COMPTECH
Jurnal Ilmu Komputer Dan Teknologi
Vol. 1 No. 2 Maret 2025, pp. 189-200
https://jurnal.compartdigital.com/index.php/comptech

peretasan dalam proses pemilu digital. Dengan meningkatnya kepercayaan publik, e-voting berbasis RSA berpotensi menjadi solusi yang lebih transparan dan efisien dibandingkan metode konvensional. Implementasi teknologi ini di masa depan dapat mendukung sistem pemilihan yang lebih modern, cepat, dan akurat tanpa mengesampingkan aspek keamanan.

DAFTAR PUSTAKA

Ahmadar, M., Perwito, P., & Taufik, C. (2021). PERANCANGAN SISTEM INFORMASI PENJUALAN BERBASIS WEB PADA RAHAYU PHOTO COPY DENGAN DATABASE MySQL. *Dharmakarya*, *10*(4), 284. https://doi.org/10.24198/dharmakarya.v10i4.35873

Ardianta Sitepu, D., & Khair MKom, H. (2022). IMPLEMENTASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDART (AES). *Jurnal Ilmiah Kaputama*, *6*(1).

Aria, M., Widodo, A., Thasandra, M., Sutra, S. O., Nasution, A. B., Ikhwan, A., Negeri, U. I., Utara, S., William, J., Ps, I. V, Estate, M., Percut, K., Tuan, S., & Serdang, D. (2023). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES. *Journal on Education*, *05*(03), 6780–6787.

Haryanto, E. V. (2021). Desain Steganografi untuk Keamanan Gambar dengan Algoritma RSA dan LSB Berbasis Android. *CSRID (Computer Science Research and Its Development Journal)*, *11*(3), 179. https://doi.org/10.22303/csrid.11.3.2019.179-190

Hermiati Reza, Indra Kaned, & Asnawati. (2020). PEMBUATAN E-COMMERCE PADA RAJA KOMPUTER MENGGUNAKAN BAHASA PEMROGRAMAN PHP DAN DATABASE MYSQL. *JURNAL MEDIA INFOTAMA*, *1*, 3–3. https://doi.org/https://doi.org/10.37676/jmi.v17i1.1317

Maharani, D., Helmiah, F., & Rahmadani, N. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, *1*(1), 1–7. https://doi.org/10.25008/abdiformatika.v1i1.130

Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation Technology (Digitech) | e*, *3*(1). https://doi.org/10.47709/digitech.v3i1.2293