JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

RSA *Blind Signature* sebagai dasar pengamanan pada sistem *e-voting* dengan Prinsip *Frictionless User*

Ellsya Nabella Nur'allifa[1,*], Rizky Rahman Judie Putra[1], Muhamad Nursalman[1]

[1]Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Ilmu Komputer, Universitas Pendidikan Indonesia, Bandung, Indonesia
Email: [1]ellsyanabella13@upi.edu, [2]rizky_rjp@upi.edu , [3]mnursalman.upi.edu@email.com
(* Email Corresponding Author: ellsyanabella13@upi.edu)
Received: 31 Juli 2025 | Revision: 31 Juli 2025 | Accepted: 31 Juli 2025

Abstrak

Sistem *e-voting (electronic voting)* telah menjadi salah satu topik penelitian penting dalam bidang keamanan informasi dan teknologi pemilu modern. Namun, berbagai studi menunjukkan bahwa sistem *e-voting* masih memiliki sejumlah kelemahan, terutama dalam aspek keamanan. Salah satu kelemahan utama yang sering disorot adalah keterlibatan langsung pemilih *(voter)* dalam proses teknis kriptografi, seperti proses *unblinding*, yang dapat menimbulkan risiko kelalaian dan kesalahan teknis. Hal ini sebagaimana dijelaskan oleh *Bartjan Wattle* dalam kutipannya *"The real security challenge lies in protecting business processes from authorized users with malicious intent or who act carelessly"*, bahwa tantangan keamanan bukan hanya datang dari penyusup eksternal, melainkan justru dari pengguna yang secara resmi diberi akses. Penelitian ini mengusulkan solusi dengan meminimalisir peran teknis voter melalui penerapan protokol *Blind Digital Signature* berbasis algoritma RSA yang seluruh proses kriptografinya mulai dari *blinding*, penandatanganan, hingga *unblinding* dilakukan oleh sistem dan pihak berwenang serta melakukan modifikasi protokol dari penelitian sebelumnya. Tujuan dari penelitian ini adalah membangun protokol *e-voting* yang mampu meminimalisir keterlibatan teknis dari pengguna *(voter)* dalam proses pengamanan sistem (*frictionless*), serta melakukan pengukuran terhadap tingkat keamanan dari protokol yang diimplementasikan. Hasil penelitian menunjukkan bahwa pengurangan peran teknis *voter* dalam proses kriptografi mampu meningkatkan keamanan dan mengurangi kesalahan, karena proses *blinding* hingga *unblinding* dikendalikan sistem. Selain itu, ditambahkan modifikasi protokol dengan melakukan tanda tangan digital saat meminta izin akses dalam komunikasi antar pihak untuk mencegah pemalsuan dan memastikan hanya entitas resmi yang dapat berpartisipasi dalam sistem.

Kata Kunci: *E-voting, User-minimalized, Frictionless, Blind Digital Signature,* RSA, *Kriptografi*

Abstract

Electronic voting (e-voting) systems have emerged as a critical research topic in the fields of information security and modern election technology. However, various studies have shown that e-voting systems still face several vulnerabilities, particularly in security aspects. One prominent weakness often highlighted is the direct involvement of voters in cryptographic technical processes, such as unblinding, which may lead to negligence and technical errors. This aligns with Bartjan Wattel's assertion that "The real security challenge lies in protecting business processes from authorized users with malicious intent or who act carelessly" indicating that threats to security do not only originate from external intruders, but often from legitimate users with access rights. This study proposes a solution to minimize the voter's technical involvement by implementing a Blind Digital Signature protocol based on the RSA algorithm, wherein the entire cryptographic process including blinding, signing, and unblinding is carried out by the system and authorized entities. The goal of the study is to develop an e-voting protocol that reduces voter participation in system security processes (frictionless), and to measure the security level of the implemented protocol. The results show that reducing the voter's technical role in the cryptographic process enhances security and minimizes errors, as the blinding to unblinding stages are controlled by the system. Moreover, the protocol is modified to include digital signatures during access requests in inter-party communications, preventing forgery and ensuring that only authorized entities can participate in the system.

Keywords: *E-voting, User-minimalized, Frictionless, Blind Digital Signature,* RSA, *Kriptografi*

1. PENDAHULUAN

Sistem *e-voting (electronic voting)* merupakan alternatif modern dalam pelaksanaan pemilihan umum di masa sekarang[1], perkembangan teknologi digital telah mendorong banyak negara dan lembaga untuk mengadopsi *sistem e-voting (electronic voting)* dalam pelaksanaan pemilu maupun pemungutan suara lainnya[2]. Di tengah meningkatnya digitalisasi dalam berbagai aspek kehidupan, *e-voting* dipandang sebagai solusi yang mampu menghemat biaya, mempercepat proses penghitungan suara, serta memperluas partisipasi pemilih melalui kanal daring atau perangkat elektronik[2]. Namun, tantangan utama dari penerapan sistem ini adalah aspek keamanan, terutama dalam menjamin anonimitas pemilih dan integritas suara[3].Salah satu masalah krusial yang sering muncul dalam sistem *e-voting* adalah risiko terjadinya kesalahan dan kelalaian yang disebabkan oleh keterlibatan user saat proses teknis berlangsung dan serangan pihak ketiga [4].

Berdasarkan permasalahan tersebut terdapat beberapa rumusan masalah dalam penelitian ini yaitu Apakah protokol *blind digital signature* dapat diimplementasikan dengan baik pada sistem pemilihan umum menggunakan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

electronic voting (*e-voting*) dengan keterlibatan *user* yang minimal dan modifikasi protokol serta bagaimana pengaruh tingkat keamanan setelah dilakukan pengurangan keterlibatan *user* dan modifikasi protokol dalam pengamanan dalam protokol *e-voting blind digital signature.* Setelah melakukan observasi terhadap beberapa penelitian lainnya terkait dengan penelitian yang dilakukan, penulis menemukan keterkaitan dengan proses yang penulis lakukan.

Penelitian yang relevan adalah karya berjudul *"Digital Signature dengan MD5 dan RSA untuk Menjaga Keaslian Data "* [5] yang mengusulkan sistem *e-voting* berbasis tanda tangan digital menggunakan algoritma RSA dan MD5, tanpa melibatkan mekanisme *blind signature*. Fokus utama penelitian ini adalah menjaga keaslian data dan validitas suara melalui proses enkripsi dan verifikasi digital, namun belum mengintegrasikan fitur anonimitas tingkat lanjut seperti yang ditawarkan oleh *blind signature*.

Kemudian penelitian berjudul "Towards Better Privacy-preserving Electronic Voting System"[6] dan "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature" [7] ini membahas mengenai modifikasi dari sistem *e-voting end-to-end verifiable* berbasis *blind signature* ,tetapi berfokus kepada metode interaksi dari *voter* terhadap sistem *e-voting.*

Selanjutnya penelitian dari jurnal "Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey" [8], "Secure and Transparent Voting Using Blind Signatures" [9], dan "Blockchain-Based E-Voting Systems: A Technology Review" [10] ini menekankan bahwa aspek usability (kemudahan dan kejelasan bagi pemilih) adalah komponen evaluasi penting, sistem ini masih menuntut keterlibatan teknis dari pemilih dalam proses kriptografi, seperti autentikasi, pengambilan token, atau interaksi dengan antarmuka yang kompleks. Sistem yang rumit atau yang menuntut banyak interaksi teknis dari pemilih cenderung berisiko lebih tinggi mengalami kesalahan pengguna, singkatnya pemilih bukan sekedar pengguna pasif, mereka adalah bagian aktif dari protokol kriptografi dan teknis.

Penelitian berikutnya dari jurnal "Implementation of e-Voting system using new blinding signature protocol" [11] penelitian ini hanya mengusulkan konsep sistem *e-voting* berbasis *blind signature* tanpa disertai implementasi atau pengujian nyata. Sistem ini masih berada pada tahap desain teoritis, dengan fokus pada skema tanda tangan dan struktur protokol, namun belum diuji secara fungsional melalui simulasi atau uji coba pengguna.

Berdasarkan hasil studi pustaka di atas, dapat dilihat bahwa GAP utama dari penelitian-penelitian sebelumnya yang meneliti mengenai sistem *e-voting* adalah masih tingginya keterlibatan teknis dari pihak *voter* yang berdampak pada peningkatan risiko keamanan dan tidak dilakukannya evaluasi keamanan pada sistem protokol yang dibangun. Oleh karena itu, penelitian ini mengusulkan modifikasi sistem protokol *blind digital signature* berbasis RSA dan mengalihkan seluruh proses teknis kriptografi pada sistem yang dikendalikan oleh panitia dan *voting center* serta melakukan tes vulnerabilitas terhadap modifikasi yang dilakukan untuk mengukur tingkat keamanan pada protokol *e-voting* yang dibangun.

Dengan pendekatan ini, keamanan sistem lebih terjaga dan risiko intervensi pengguna yang tidak sah dapat diminimalkan (*frictionless*) [12]. Tujuan dari penelitian ini adalah membangun sebuah protokol *e-voting* yang meminimalisir keterlibatan pengguna/*user* dalam penggunaannya sesuai dengan teori *Bartjan Wattel*, serta mendapatkan hasil pengukuran tingkat keamanan pada modifikasi protokol *e-voting* yang dibangun.

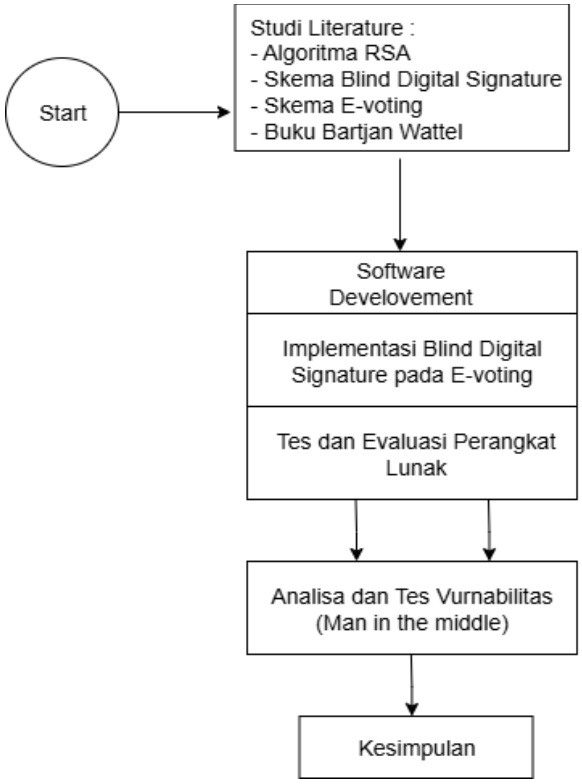
2. METODOLOGI PENELITIAN

Metodologi yang dipakai adalah metode pengumpulan data dan metode pengembangan perangkat lunak menggunakan model air terjun *(waterfall)* yang berurutan mulai dari *analysis architecture, design architecture, implementation,* dan *testing*.

2.1 Desain Penelitian

Dalam konteks pengembangan sistem *e-voting* berbasis *blind digital signature* menggunakan algoritma RSA, desain penelitian ini mencakup tahapan analisis kebutuhan sistem seperti perancangan arsitektur, alur kerja sistem, implementasi algoritma kriptografi, hingga pengujian dan evaluasi keamanan serta fungsionalitas sistem. Setiap tahapan dirancang secara sistematis untuk memastikan bahwa solusi yang dibangun dapat menyelesaikan permasalahan yang ada. Gambaran umum mengenai desain penelitian yang akan dilakukan ditujukan pada gambar dibawah ini :

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527



Gambar 1. Desain penelitian

2.2 Studi Literatur

informasi dan data yang akurat sangat dibutuhkan untuk menunjang proses penelitian[13]. Penulis berusaha mendapatkan data yang akurat dan mampu menunjang penelitian. Proses studi literatur dilakukan untuk mendalami pengetahuan tentang *e-voting*, *digital signature, blind digital signature*, dan *algoritma* RSA melalui jurnal, buku dan penelitian sebelumnya yang didapatkan melalui perpustakaan dan internet.

2.3 RSA

RSA adalah *algoritma enkripsi* kunci publik, a*lgoritma* ini pertama kali diadaptasi untuk membuat tanda tangan digital [14]. Saat ini *algoritma* RSA merupakan *algoritma* yang paling sering digunakan di antara *algoritma* kunci publik lainnya. *Algoritma* ini menggunakan pasangan kunci, kunci publik dan kunci privat, sehingga memungkinkan komunikasi yang aman antara dua pihak tanpa perlu berbagi kunci privat [15]. RSA juga digunakan untuk menandatangani dan memverifikasi integritas pesan secara digital, memastikan bahwa pesan tersebut tidak diubah oleh pihak ketiga. Variasi aplikasi RSA sangat luas, mulai dari keamanan data hingga keamanan komunikasi, dan merupakan komponen penting dari banyak protokol keamanan Internet yang umum digunakan [16].

2.4 *Blind Digital Signature*

Blind digital signature adalah suatu bentuk tanda tangan digital yang memungkinkan seseorang menandatangani pesan atau dokumen elektronik tanpa mengetahui isinya. Ini adalah teknik enkripsi yang digunakan untuk melindungi privasi dan *anonimitas* pengguna selama transaksi atau komunikasi *online* [17]. Penggunaan tanda tangan buta sering dikaitkan dengan aplikasi yang memerlukan keamanan atau *anonimitas*, seperti sistem pemungutan suara elektronik, sistem pembayaran digital, atau protokol keamanan teknologi *blockchain*. Dengan menggunakan teknik ini, pengguna dapat memastikan keabsahan tanda tangan digital tanpa mengungkapkan isi pesan asli kepada penyedia tanda tangan [18]. Salah satu keunggulan utamanya adalah privasi pengguna, dimana pengguna yang meminta tanda tangan dapat menjaga kerahasiaan isi pesan yang akan ditandatangani. Hal ini berguna dalam situasi di mana privasi pesan merupakan aspek penting, seperti dalam sistem pemungutan suara atau kredensial anonim. Keunggulan lainnya adalah kemampuan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

memverifikasi tanda tangan dengan mudah tanpa mengetahui isi pesan, sehingga penerima pesan dapat memastikan keabsahannya [19].

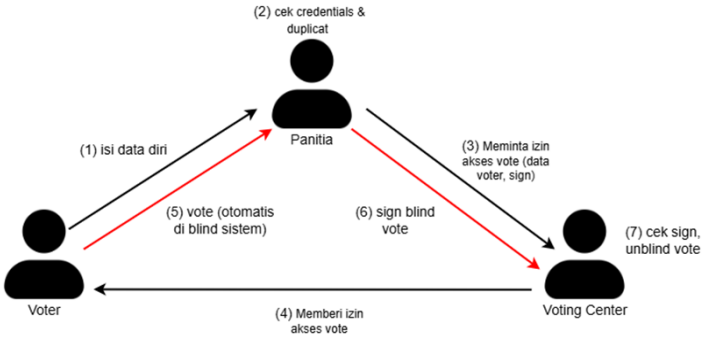
2.5 Vulnerabilitas Tes

Vulnerabilitas test atau pengujian kerentanan adalah proses yang dilakukan untuk mengidentifikasi dan menilai kerentanan dalam sistem atau aplikasi. Salah satu bentuk pengujian kerentanan adalah *man in the middle (MITM) attack*. *Man in the middle attack* adalah jenis serangan *cyber* di mana penyerang menyusup di antara dua pihak yang sedang berkomunikasi. Penyerang dapat memantau, menyadap, bahkan memodifikasi data yang dipertukarkan di antara kedua pihak tanpa mereka sadari. Serangan ini berbahaya karena memungkinkan penyerang mencuri informasi sensitif seperti kredensial login, nomor kartu kredit, atau data pribadi lainnya [20].

3. HASIL DAN PEMBAHASAN

3.1 Desain Arsitektur

Desain arsitektur ini menjelaskan tentang bagaimana gambaran terjadinya proses implementasi RSA pada protokol *blind digital signature* untuk sistem *e-voting*, dengan berbagai perubahan, penambahan dan pengurangan fungsi atau peran setiap orang maupun sistem yang dibangun. Berikut merupakan gambaran dari langkah dalam prosesnya



Gambar 3.Desain arsitektur

Ada modifikasi terhadap skema protokol dari penelitian sebelumnya, dimana modifikasi ini menambahkan penyertaan tanda tangan digital pada proses panitia meminta izin akses *vote* kepada *voting center,* supaya mencegah terjadinya campur tangan dari pihak luar dan memastikan hanya panitia yang sah yang terlibat.

3.2 Implementasi Blind Digital Signature pada E-voting

1. **Proses Voter Memasukkan Data Diri**

   Voter memasukan data diri untuk dikirim dan diperiksa oleh panitia, dan panitia memeriksa data tersebut dengan memeriksa *credentials* nya dan juga memastikan tidak ada duplikat data. Agar memastikan bahwa *voter* hanya bisa mendapatkan satu kali kesempatan untuk memilih. Pada penelitian ini peran *voter* di minimalisir, jadi *voter* hanya melakukan pendaftaran dan *voting* saja.

2. **Proses Memperoleh Izin Akses Voting**

   Setelah memeriksa data *voter*, panitia meminta izin *vote* kepada *voting center* untuk *voter* dengan membawa data *voter* dan tanda tangan nya agar *voter* bisa melakukan *voting*, setelah valid maka *voting center* memberi akses langsung kepada *voter* agar dapat langsung memilih (*voting*). Penelitian ini juga melakukan modifikasi protokol dengan menambahkan tanda tangan pada proses ini agar hanya pihak yang sah saja yang dapat terlibat.

3. **Proses Voting dan Tandatangan**

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

Setelah akses diberikan, maka *voter* langsung melakukan *voting*, yang kemudian *voting* tersebut di *blind*, hasil *blind vote* tersebut langsung diserahkan kepada panitia untuk di cek, setelah diperiksa dan valid maka panitia akan menandatangani *blind vote* tersebut. Kemudian *blind vote* yang telah ditandatangani langsung dikirimkan ke *voting center.*

4. **Proses Cek Signature dan Unblind**

   Voting center memeriksa tanda tangan untuk memastikan bahwa tanda tangan tersebut berasal dari panitia, lalu setelah tanda tangan valid *voting center* akan membuka buta dari pesan yang kemudian pesan asli tersebut akan dihitung dan dimasukkan kedalam rekap perhitungan suara.

3.3 Modifikasi Skema Blind Digital Signature

Dalam penelitian ini, dilakukan modifikasi pada skema dengan memindahkan proses *unblind* dari pihak *voter* ke *voting center* serta modifikasi protokol dengan menambahkan tanda tangan pada saat proses minta izin akses *vote* agar hanya pihak yang asli saja yang dapat terlibat. Perubahan ini bertujuan untuk keamanan sistem dan mencegah resiko kesalahan serta kelalaian yang mungkin terjadi oleh pengguna (*voter*). Dalam arsitektur yang baru ini tugas *voter* hanyalah mengisi data diri dan membuat pilihan saja. Untuk memahami bagaimana protokol yang diusulkan bekerja secara teknis, berikut ini akan menjelaskan tahapan proses matematika kriptografi yang menjadi inti dari sistem, mulai dari pembangkitan kunci, proses *blinding*, penandatanganan digital, validasi tanda tangan (*signature verification*), hingga proses *unblinding* [21].

1. **Pembangkitan kunci publik dan kunci privat RSA**
   - `Pilih 2 bilangan prima, p,q dengan p ≠ q, misalkan p = 1301 dan q = 1607`
   - Hitung nilai n dimana n = p x q sehingga n = 1301 x 1607 = 2090707
   - Hitung nilai Φ(n), dimana Φ(n) = (p – 1) (q – 1) sehingga didapat Φ(n) = 1300 x 1606 = 2087800
   - Cari nilai e minimal, sedemikian sehingga e relatif prima terhadap Φ(n) dan relatif prima terhadap n dengan syarat 1 < e < Φ(n), sehingga diperoleh e = 7
   - Cari nilai d bilangan bulat sedemikian sehingga e.d mod Φ(n) = 1
   - atau d= (1+k.Φ(n))/e , nilai d dapat dicari dengan mencoba nilai k =1, 2, 3,…. Sehingga diperoleh d bilangan bulat.
2. **Membutakan pesan (blinding)**

$$M' = (M \cdot r\ \mathrm{e}) \bmod n \qquad (1)$$

3. **Menandatangani pesan yang dibutakan (signing)**

$$S' = (M')\mathrm{d} \bmod \mathrm{n} \qquad (2)$$

4. **Verifikasi Signature**

$$S = (S' \cdot r\ \text{-}1) \bmod n \qquad (3)$$

5. **Membuka buta pesan (unblinding)**

$$M = S\mathrm{e} \bmod n \qquad (4)$$

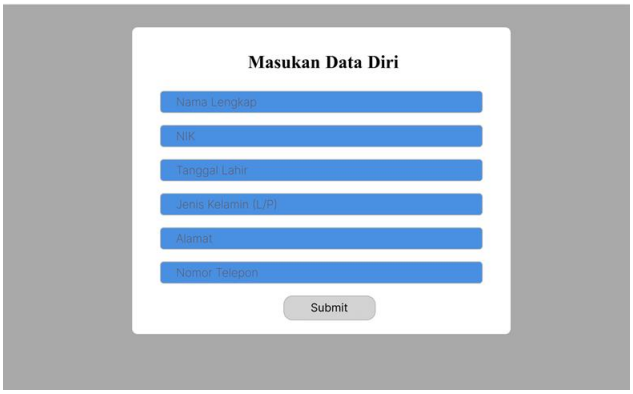
3.4 Perancangan Antarmuka

Pada *e-voting* sebelumnya masih bersifat konsep, sementara *e-voting* ini dalam bentuk prototype perangkat lunak maka dibutuhkan suatu perancangan antarmuka untuk implementasinya[22].

1. Halaman untuk pemilih (*voter*)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

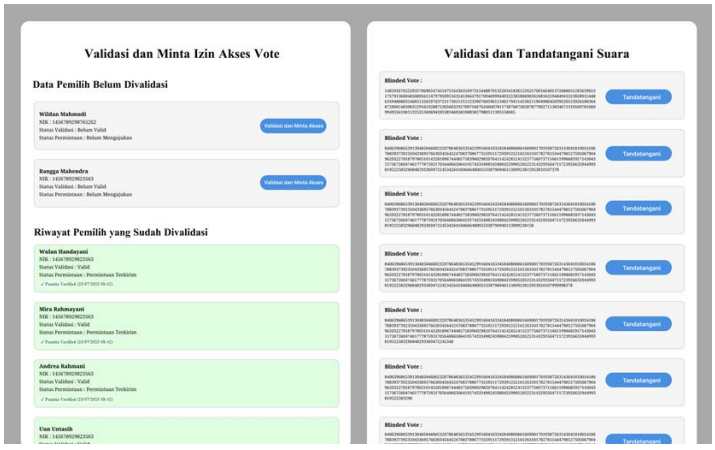
Halaman ini digunakan oleh pemilih untuk melakukan pendaftaran dengan mengisi data, setelah mendaftar pemilih akan menunggu validasi dari panitia. Jika akses telah diberikan oleh *voting center,* pemilih akan mendapatkan *notifikasi* dan dapat masuk ke halaman *voting* untuk memberikan suaranya.



Gambar 4.Halaman input data voter

2. Halaman panitia

Halaman ini digunakan oleh panitia untuk memverifikasi data pemilih yang masuk, setelah data divalidasi panitia dapat mengirim permintaan akses kepada *voting center* agar pemilih tersebut dapat memberikan suara. Selain itu, panitia juga menerima dan menandatangani suara buta (*blind vote*) yang dikirim oleh pemilih sebelum diteruskan ke *voting center.*

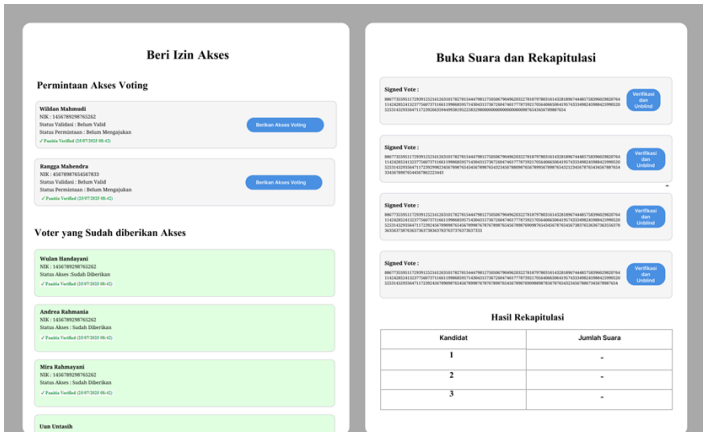


Gambar 5 Halaman panitia

3. Halaman voting center

Halaman ini berfungsi untuk mengelola permintaan akses dari panitia, *voting center* akan memberikan izin kepada pemilih untuk melakukan *voting*. Selain itu, *voting center* juga bertugas memverifikasi keaslian tanda tangan digital pada suara yang masuk dari panitia, melakukan proses *unblinding*, dan melakukan rekap suara yang sah.

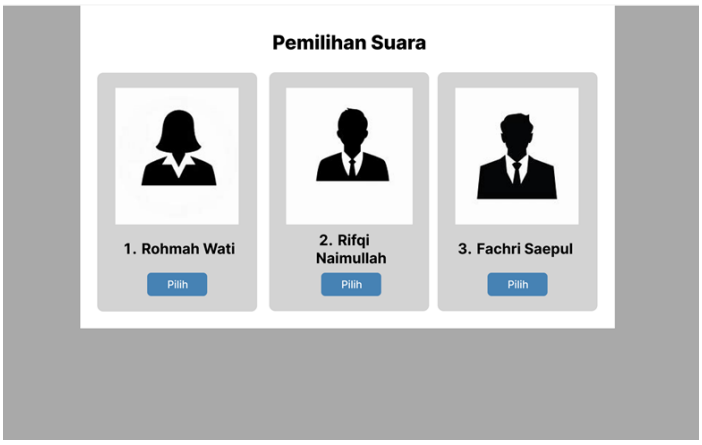
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527



Gambar 6.Halaman voting center

4. Halaman voting

   Halaman ini adalah tempat bagi pemilih yang telah mendapatkan akses untuk memberikan suaranya, pemilih akan melihat daftar kandidat dan memilih satu di antaranya. Setelah memilih suara akan dibutakan, lalu dikirim ke panitia untuk proses penandatanganan dan validasi.



Gambar 7.Halaman voting

3.5 Tes dan Evaluasi Perangkat Lunak

Berikut adalah skenario pengujian perangkat lunak untuk sistem *e-voting* menggunakan metode *Black Box Testing* dalam bentuk tabel yang memungkinkan pengguna lebih mudah melihatnya [23].

Tabel 1.Black box testing

No	Langkah Uji	Hasil yang Diharapkan	Hasil Pengujian	Status
1.	**Input Data Pendaftaran (Nama, NIK, tanggal lahir,**	Data pendaftaran diterima dan pemilih didaftarkan dengan sukses	Data *voter* disimpan ke database	Berhasil

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

	jenis kelamin, alamat dan nomor telepon			
2.	**Pengecekan Data**	Data pemilih diizinkan melanjutkan ke tahap berikutnya	Data *voter* yang valid dapat lanjut ke proses berikutnya	Berhasil
3.	**Minta Izin Akses *Vote***	Panitia mengirim permintaan izin akses ke *voting center* dan menerima respons yang sesuai	Panitia mengirim permintaan akses vote dan *voting center* menerima izin tersebut	Berhasil
4.	**Memberi Izin Akses *Vote***	Pemilih menerima izin akses dan dapat melanjutkan ke tahap pemungutan suara	Pemilih (*voter*) menerima izin akses dan dapat melanjutkan ke tahap pemungutan suara	Berhasil
5.	**Pemungutan Suara (*voting*)**	Suara diterima dan tercatat dalam sistem	Suara diterima dan terbutakan oleh bilangan acak dan suara telah disimpan ke database	Berhasil
6.	**Pengecekan Data Setelah *voting***	Data valid dan sesuai dengan data sebelumnya	Data valid dan sesuai dengan data sebelumnya	Berhasil
7.	**Tandatangan**	Tandatangan diterima dan dicatat dalam sistem	Tandatangan diterima dan dicatat dalam sistem yang tersimpan ke database	Berhasil
8.	**Cek Tanda Tangan**	Tanda tangan diterima dan pemilih dapat melanjutkan ke proses berikutnya	Tanda tangan diterima dan disimpan ke database sehingga pemilih dapat melanjutkan ke proses berikutnya	Berhasil
9.	**Unblinding**	Suara diungkapkan dengan benar dan tercatat dalam sistem	Suara diungkapkan dengan benar dan tercatat dalam sistem yang tersimpan ke database	Berhasil
10.	**Perhitungan Suara**	Hasil perhitungan sesuai dengan data suara yang masuk dan ditampilkan dengan benar	Hasil perhitungan sesuai dengan data suara yang masuk dan ditampilkan dengan benar	Berhasil

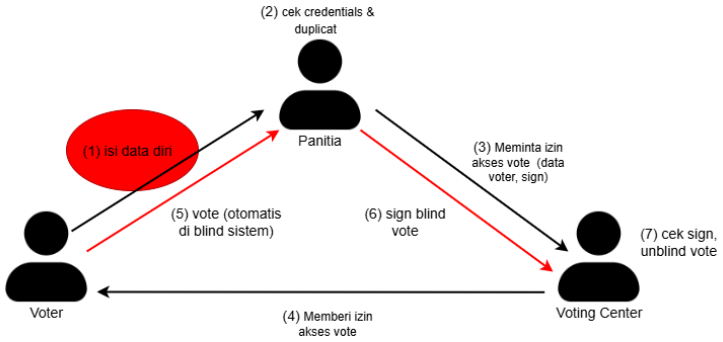
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

3.6 Analisis dan Tes Vurnabilitas (Man in the middle)

Tes keamanan ini menggunakan metode *man in the middle* (MITM) dengan beberapa skenario yang mungkin terjadi diantara ketiga peran yaitu *voter*, panitia dan *voting center* [24]. Berikut beberapa skenario yang mungkin terjadi.

1. MITM antara Voter dan Panitia

Dalam serangan *Man in the Middle* (MITM), penyerang dapat menggunakan identitas yang sudah dipakai atau data diri palsu saat dikirim dari *voter* ke panitia. Identitas *voter* asli tergantikan oleh data palsu, yang memungkinkan terjadinya duplikasi pemilih atau manipulasi basis data. Untuk mencegah hal ini, sistem memverifikasi apakah NIK sudah pernah digunakan. Jika ditemukan NIK ganda, sistem akan secara otomatis menolak pendaftaran dan menampilkan pesan ke panitia bahwa "NIK sudah terdaftar dalam sistem." Dengan ini, penyusup akan gagal melakukan pendaftaran ganda. Pada penelitian sebelumnya juga *voter* memiliki peran dalam proses teknisnya yaitu melakukan *unblinding* sehingga rentan mengalami risiko kesalahan dan kelalaian dalam prosesnya, perbaikan pada penelitian ini adalah mengalihkan seluruh proses teknis yang sebelumnya dilakukan *voter* kini dilakukan oleh sistem dan pihak yang berwenang, ini bisa menghilangkan risiko kesalahan pengguna serta menjaga keamanan protokol. Berikut gambaran dimana letak penyerangan bisa terjadi.

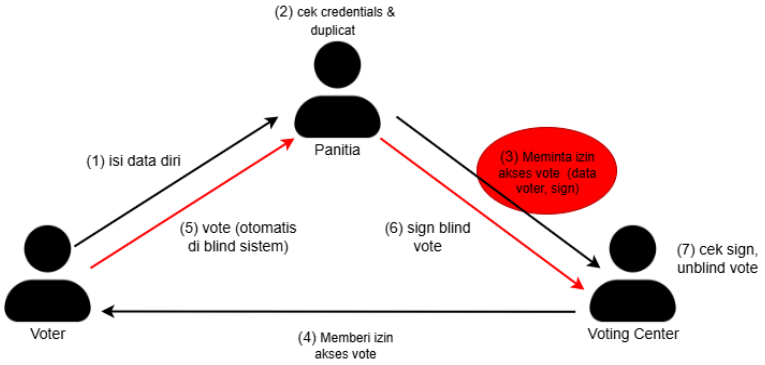


Gambar 8. Serangan dari voter ke panitia

2. MITM antara Panitia dan Voting Center

Salah satu potensi serangan bisa terjadi saat panitia meminta izin akses *vote* kepada *voting center*. Setelah data *voter* divalidasi oleh panitia, panitia akan mengirimkan permintaan akses *voting* ke *voting center*. Untuk menjamin keaslian permintaan tersebut, pengiriman izin akses ini disertai dengan tanda tangan digital yang dihasilkan menggunakan kunci privat panitia. *Voting center* kemudian memverifikasi apakah tanda tangan tersebut valid dan benar berasal dari panitia asli, dengan menambahkan modifikasi protokol menggunakan tanda tangan digital dalam proses ini dapat mencegah serangan dari panitia palsu. Pada skenario MITM, penyerang mencoba berpura-pura menjadi panitia dengan mengirimkan permintaan akses ke *voting center*, namun menggunakan kunci palsu. Karena sistem memverifikasi tanda tangan digital tersebut, maka sistem akan langsung mendeteksi bahwa tanda tangan tidak valid dan bukan berasal dari panitia dengan menolak permintaan dan mencatat log potensi serangan tersebut. Berikut gambaran dimana letak penyerangan bisa terjadi.

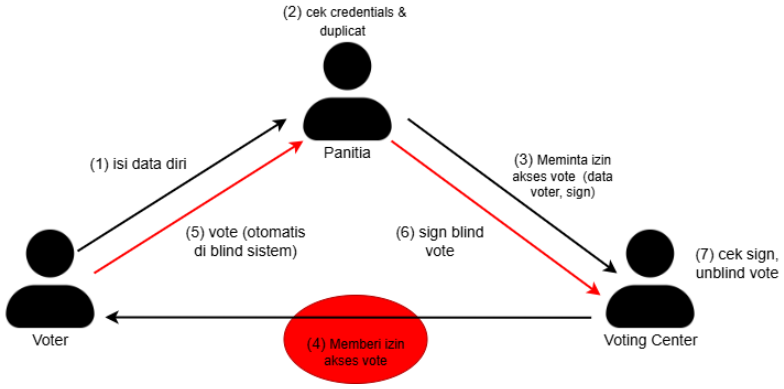
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527



Gambar 9.Serangan dari panitia ke voting center

3. MITM antara Voting Center dan Voter

Setelah permintaan panitia diverifikasi dan disetujui, *voting center* memberikan akses kepada *voter* dengan menampilkan tautan (*link*) menuju halaman *voting* di halaman *voter*. Tautan ini hanya akan muncul jika proses validasi berhasil dan akses resmi telah diberikan. Dalam serangan MITM, penyusup berpura-pura menjadi *voting center* dan mencoba mengirim akses palsu kepada *voter*. Namun karena *voting center* yang palsu tidak memiliki kunci autentik atau tanda tangan sah dari sistem, maka sistem akan menolak dan tidak akan menampilkan tautan *voting* di halaman *voter* serta mencatat log potensi serangan tersebut. Berikut gambaran dimana letak penyerangan bisa terjadi.



Gambar 10.Serangan dari voting center ke voter

4. KESIMPULAN

Berdasarkan hasil penelitian yang dikaji, maka dapat disimpulkan ada dua poin utama yang menjadi kesimpulan yaitu pengurangan peran teknis *voter* (*frictionless*) dalam proses kriptografi terbukti dapat meningkatkan keamanan dan mengurangi potensi kesalahan, karena seluruh proses teknis kini dikendalikan oleh sistem dan pihak berwenang. Serta penggunaan metode RSA dan modifikasi protokol *blind digital signature* dengan penambahan tanda tangan digital pada proses permintaan akses dari panitia ke *voting center* memberikan kontrol keamanan, sehingga sistem hanya menerima komunikasi dari entitas yang sah dan memblokir kemungkinan serangan pemalsuan atau penyusupan. Dengan demikian, penelitian ini mereduksi resiko keamanan dalam sisi kelalaian pengguna pada sistem *e-voting* berbasis *blind digital signature* melalui penguatan protokol keamanan dan penyederhanaan peran pengguna tanpa mengurangi fungsionalitas utama sistem.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527

REFERENCES

[1] G. Ikrissi and T. Mazri, "Electronic Voting: Review and Challenges," Electronic Voting: Review and Challenges, Springer International Publishing, 2024, pp. 110–119. doi: 10.1007/978-3-031-53824-7_11.

[2] P. Lohakare, "Online voting system," *Proceedings*, 2024, pp. 646–649. doi: 10.69758/scel2919.

[3] A. W. W. Hameed, "A Secure Electronic Voting," IGI Global, 2011, pp. 431–449. doi: 10.4018/978-1-61520-789-3.CH032.

[4] R. A. Cordery, M. J. Campagna, and B. Haas, "Electronic voting system and associated method," U.S. Patent US20090032591A1, Jan. 29, 2009.

[5] B. K. Hutasuhut, S. Efendi, dan Z. Situmorang, "Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 3, no. 2, pp. 101–109, Mar. 2019.

[6] Z. Yan, Z. Jiang, dan Y. Li, "Towards Better Privacy-preserving Electronic Voting System," *arXiv preprint*, arXiv:2205.12094, May 2022.

[7] M. Kumar, S. Chand, dan C. P. Katti, "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, Jun. 2020. doi: 10.1109/JSYST.2019.2940474.

[8] M. P. Heinl, S. Gölz, dan C. Bösch, "Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey," *ACM Computing Surveys*, vol. 55, no. 8, Art. no. 167, Dec. 2022. doi: 10.1145/3551386.

[9] P. Rupa, R. Usha, R. Himaja, dan A. Kavya, "Secure and Transparent Voting using Blind Signatures," *International Journal of Scientific Research in Engineering and Management (IJSREM)*, vol. 9, no. 6, pp. 1–6, Jun. 2025.

[10] M. H. Berenjestanaki, H. R. Barzegar, N. El Ioini, dan C. Pahl, "Blockchain-Based E-Voting Systems: A Technology Review," *Electronics*, vol. 13, no. 1, Art. no. 17, Dec. 2023. doi: 10.3390/electronics13010017.

[11] P. Kuppuswamy dan O. S. A. Al-Mushayt, "Implementation of e-Voting system using new blinding signature protocol," *IOSR Journal of Computer Engineering*, vol. 8, no. 4, pp. 36–40, Jan.–Feb. 2013.

[12] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, "A frictionless and secure user authentication in web-based premium applications," *IEEE Access*, vol. 9, pp. 129240–129255, 2021.

[13] P. Chen, "Data Acquisition System based on Serial Port," *Journal of Theory and Practice of Engineering Science*, vol. 4, no. 3, pp. 87–98, 2024. doi: 10.53469/jtpes.2024.04(03).09.

[14] T. Raharjoeningroem and M. Aria, "Studi dan implementasi algoritma RSA untuk pengamanan data transkrip akademik mahasiswa," *Majalah Ilmiah UNIKOM*, vol. 8, no. 1, pp. 77–90, 2011.

[15] A. Wahyuni, "Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid: Diffie-Hellman dan RSA," *Majalah Ilmiah Informatika*, vol. 2, no. 2, 2011.

[16] Z. Arifin, "7 Program Studi Ilmu Komputer Universitas Mulawarman," *Jurnal Informatika Mulawarman*

[17] W. I. Rahmawati, "Pemanfaatan protokol blind signature dalam hal pengesahan dokumen yang dilakukan seorang notaris pada jasa pelayanan notaris digital," *Konferensi Nasional Teknologi Informasi & Aplikasinya (KNTIA)*, vol. 3, 2016.

[18] T. G. Limandra, "Implementasi blind signature dalam melakukan electronic voting," *Makalah Kriptografi IF5054*, Institut Teknologi Bandung, 2007.

[19] S. Wang, Y. H., and L. D., *Proceedings of 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC 2018)*, Chongqing, China, Oct. 12–14, 2018, IEEE.

[20] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed," *arXiv: Cryptography and Security*, 2021.

[21] N. H. Sari, "Penerapan Teknik Digital Signature Dalam Pengamanan Piagam Penghargaan Menggunakan Algoritma SHA-1 dan RSA," *Management of Information System Journal*, vol. 2, no. 3, pp. 55–67, 2024.

[22] A. Mursyidah, I. Aknuranda, and H. M. Az-Zahra, "Perancangan Antarmuka Pengguna Sistem Informasi Prosedur Pelayanan Umum Menggunakan Metode Design Thinking (Studi Kasus: Fakultas Ilmu Komputer Universitas Brawijaya)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 4, pp. 3931–3938, 2019.

[23] E. V. Nugraha, R. Y. Ariyana, and E. K. Nurnawati, "Uji Black Box Tes Aplikasi Software Development System Information (SODEVI) PT. Dimata Sora Jayate Menggunakan Katalon Studio," *PROSIDING SNAST*, pp. E60–E65, 2022.

[24] F. Alwafi, "Analisis dan Implementasi Keamanan Jaringan pada PT. Dae Myung Highness Indonesia," *Penelitian Ilmu Komputer Sistem Embedded dan Logic*, vol. 3, no. 1, pp. 1–10, 2015.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 782-793
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.527