

Integrated Cryptographic Framework berbasis AES-256, RSA-2048, dan Blind Signature untuk Secure E-Voting Model

Justin Matthew Triono¹, Eko Hari Rachmawanto^{2*}, Azriel Sebastian Pamungkas³, Budi Handoko⁴

Department of Informatics Engineering, Universitas Dian Nuswantoro

111202314877@mhs.dinus.ac.id¹, eko.hari@dsn.dinus.ac.id², 111202314868@mhs.dinus.ac.id³, handoko@dsn.dinus.ac.id⁴

Article Info

Article history:

Received 2026-07-10

Revised 2026-08-10

Accepted 2026-10-03

Keyword:

*Electronic voting,
AES,
RSA,
3DES,
Blind Signature.*

ABSTRACT

Electronic voting (e-voting) is presented as a digital solution to replace the conventional election system where the process of recording, storing, and calculating voter vote data will be done digitally, with the aim of accelerating the vote recapitulation process and minimizing human errors. In its implementation, strict security guarantees are required for crucial aspects such as voter anonymity and vote integrity from manipulation in its implementation. To address these challenges, this study proposes a network-based e-voting model integrated with four cryptographic pillars: the AES-256 algorithm used to encrypt vote data symmetrically and ensure the confidentiality of each individual's choices efficiently; the RSA-2048 algorithm, an asymmetric cryptographic system used to secure AES key exchange and provide authentication for each data transaction; and the Blind Signature scheme that allows the server to verify and sign votes without knowing their contents, thus effectively separating the voter's identity from his or her choice. Experimental results show that the proposed system successfully meets five fundamental security properties: anonymity (deanonymization probability $\approx 1/2^{2048} \approx 3.23 \times 10^{-617}$), integrity (100% manipulation detection rate via HMAC-SHA256), confidentiality (via AES-256-CBC double encryption), legitimacy (via voter registration verification), and singleness (100% prevention of duplicate voting). Performance evaluations show an average processing time of 763 milliseconds per voter, confirming that the level of cryptographic security does not compromise the overall system responsiveness. With this architecture, the proposed model not only promises a more efficient election process but also increases the level of public trust through a transparent and cryptographically secure system.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. PENDAHULUAN

Pemilihan umum merupakan pilar utama dalam sistem demokrasi dengan tujuan memilih pemimpin secara jujur dan adil guna menjamin partisipasi seluruh warga negara dalam pembangunan bangsa [11]. Seiring meluasnya penggunaan teknologi informasi, electronic voting (e-voting) hadir sebagai solusi digital untuk menggantikan sistem konvensional demi menyederhanakan prosedur birokrasi dan meminimalisir kesalahan manusia [13]. Implementasi teknologi dalam proses pemungutan suara digital ini diharapkan dapat mempercepat proses rekapitulasi serta meningkatkan aksesibilitas bagi masyarakat luas [4]. Dalam pelaksanaannya, sistem ini memerlukan jaminan keamanan

data yang terukur terhadap aspek krusial seperti integritas suara dari berbagai ancaman manipulasi siber. Sebagai bentuk implementasi pengamanan data dalam aplikasi e-voting, sistem keamanan modern memanfaatkan kombinasi algoritma kriptografi simetris dan asimetris untuk mengamankan data sejak awal pengiriman hingga penyimpanan di basis data [9].

Protokol kriptografi blind signature berperan sebagai instrumen vital untuk mewujudkan anonimitas total di mana identitas pemilih secara teknis terputus dari pilihan suara [8]. Mekanisme ini bekerja dengan memungkinkan pemilih untuk memberikan faktor pembuta (blinding factor) pada data suaranya sebelum dikirimkan kepada otoritas penyelenggara guna mendapatkan tanda tangan digital. Hal ini memungkinkan otoritas untuk memberikan validasi

keabsahan hak pilih secara sistematis tanpa pernah mengetahui isi pilihan di dalam surat suara tersebut [12]. Setelah divalidasi, proses unblinding dilakukan guna menghapus faktor pembuta sehingga menghasilkan surat suara digital sah tanpa jejak audit yang menghubungkan suara ke pengirim aslinya [8]. Agar surat suara anonim yang telah disahkan ini tetap terjaga kerahasiaan isinya saat disimpan dan dihitung, sistem membutuhkan perlindungan enkripsi lanjutan dengan menggunakan algoritma AES-256 [9].

Algoritma AES-256 (Advanced Encryption Standard) secara efisien digunakan untuk mengenkripsi isi data suara secara simetris serta memastikan kerahasiaan pilihan setiap individu pada tingkat basis data. Implementasi algoritma AES dalam keamanan data e-voting ini terbukti mampu memperkuat sistem perlindungan terhadap akses ilegal dari pihak luar melalui proses matematis yang kompleks [13]. Peran utama enkripsi simetris ini adalah menawarkan kecepatan pemrosesan data bervolume tinggi tanpa mengorbankan tingkat keamanan privasi bagi para pengguna. Melalui penerapan AES, detail informasi pilihan pemilih yang dikirimkan melalui jaringan akan terlindungi dari potensi penyadapan oleh pihak-pihak yang tidak bertanggung jawab [9]. Untuk mendistribusikan kunci rahasia AES tersebut secara aman menuju server sentral, sistem memerlukan tambahan keamanan asimetris tangguh yang disediakan oleh algoritma RSA [13].

Algoritma RSA 2048 merupakan sistem kriptografi asimetris yang dimanfaatkan secara spesifik untuk mengamankan pertukaran kunci AES dan memberikan autentikasi terhadap setiap transaksi data. Ketahanan matematis dari algoritma RSA menjadi pondasi utama dalam mendukung protokol blind signature untuk menciptakan sistem yang terukur dan terpercaya [8]. Melalui manajemen kunci publik dan privat yang sistematis, sistem dapat menjamin bahwa hanya entitas yang sah yang dapat memverifikasi keabsahan data pemilu. Penggunaan enkripsi asimetris ini sangat krusial untuk membangun tingkat kepercayaan pemilih terhadap keandalan dan integritas sistem e-voting secara keseluruhan [12].

Beberapa penelitian terkait telah mengusulkan penggunaan teknologi desentralisasi hibrida berbasis awan untuk meningkatkan keamanan sistem pemilihan elektronik secara transparan [1]. Metode lain juga mengeksplorasi integrasi antara sistem komputasi terdistribusi dengan teknik machine learning guna menciptakan mekanisme pemungutan suara yang lebih aman dan terjamin [2]. Selain itu, terdapat studi yang mengkombinasikan teknologi basis data terenkripsi sumber terbuka dengan fitur autentikasi wajah untuk memperkuat performa perlindungan AES dan RSA [18]. Meskipun demikian, efektivitas sistem pemilihan digital sangat bergantung pada ketahanan infrastrukturnya terhadap berbagai jenis serangan siber yang kian dinamis [3].

Berdasarkan kajian literatur tersebut, terdapat beberapa kesenjangan penelitian (research gap) yang perlu diatasi. Pertama, sebagian besar studi [1], [2], [18] masih mengandalkan pendekatan terpusat tanpa mekanisme

pemisahan identitas yang kuat antara pemilih dan suaranya. Kedua, penelitian yang ada umumnya belum mengintegrasikan secara simultan tiga lapisan keamanan—pemisahan identitas (Blind Signature), kerahasiaan data (AES-256), dan distribusi kunci aman (RSA-2048)—dalam satu arsitektur yang terukur. Ketiga, belum ada studi yang secara empiris mengukur trade-off antara tingkat keamanan kriptografi dan performa sistem pada skala pemilih yang bervariasi.

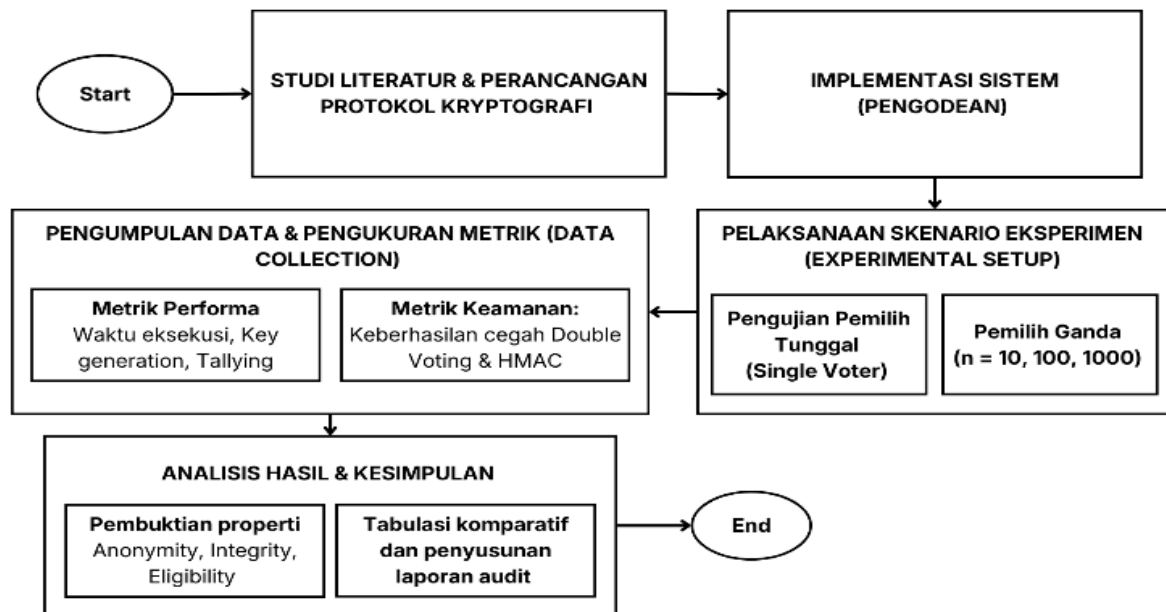
Pemilihan kombinasi algoritma dalam penelitian ini didasarkan pada prinsip defense-in-depth dan saling melengkapi (complementary security functions). RSA Blind Signature dipilih karena secara matematis mampu memutus keterkaitan identitas pemilih dari pilihan suara (unlinkability), sebuah properti yang tidak dapat disediakan oleh enkripsi simetris maupun asimetris konvensional [8]. AES-256 dipilih karena efisiensi komputasinya dalam mengenkripsi data bervolume besar serta ketahanannya terhadap serangan brute-force dengan ruang kunci 2^{256} [9]. Sementara itu, RSA-2048 berfungsi sebagai mekanisme distribusi kunci aman dan autentikasi transaksi, yang tidak dapat dipenuhi oleh skema simetris murni [12]. Kombinasi ini dipilih karena setiap algoritma menutupi kelemahan algoritma lainnya: AES menawarkan kecepatan, RSA menyediakan distribusi kunci yang aman, dan Blind Signature menjamin anonimitas—sebuah sinergi yang belum banyak dieksplorasi dalam penelitian e-voting sebelumnya.

Berdasarkan tantangan dan kesenjangan tersebut, penelitian ini mengembangkan sebuah Model E-Voting Berbasis Jaringan dengan mengintegrasikan kombinasi algoritma AES-256, RSA-2048, dan Blind Signature. Sistem ini dirancang agar setiap algoritma saling melengkapi, di mana blind signature berfungsi memutus tautan identitas pemilih dari suaranya secara mutlak. Selanjutnya, surat suara yang telah menjadi anonim tersebut dienkripsi menggunakan efisiensi algoritma simetris AES-256 guna memastikan kerahasiaan isi pilihan secara terukur di dalam basis data. Kekuatan AES ini kemudian disempurnakan oleh algoritma asimetris RSA 2048 yang berperan vital dalam melindungi proses distribusi kunci enkripsi agar seluruh transaksi data tetap autentik [12]. Melalui integrasi algoritma hibrida ini, validitas data dapat dibuktikan secara matematis sehingga mampu menghasilkan model pemilu yang transparan dan menjamin privasi secara terstruktur.

II. METODE

A. Alur Penelitian

Penelitian ini dilaksanakan sebagai sebuah proof-of-concept eksperimental untuk menguji implementasi protokol kriptografi canggih dalam konteks sistem pemilihan elektronik (e-voting). Berbeda dengan pengembangan aplikasi pada umumnya, fokus utama dari kerangka penelitian ini adalah menguji properti keamanan teknis secara matematis dan empiris, daripada berfokus pada aspek usability atau antarmuka pengguna. Rangkaian tahapan pengerjaan penelitian ini diilustrasikan pada Gambar 1.



Gambar 1. Alur Tahapan Penelitian

Untuk menjamin penelitian berjalan secara terstruktur dan teratur, setiap tahapan pada diagram di atas dijabarkan sebagai berikut:

1) Studi Literatur dan Perancangan Protokol Kriptografi

Tahap ini difokuskan pada kajian matematis dan pembuktian teoritis atas algoritma yang digunakan. Peneliti merancang protokol keamanan yang terdiri dari RSA Blind Signature untuk memisahkan identitas pemilih dari suaranya (unlinkability), AES-256-CBC dengan HMAC-SHA256 untuk kerahasiaan dan integritas, serta RSA-2048 untuk lapisan enkripsi transportasi (Transport Encryption). Pada tahap ini juga dirancang 7 (tujuh) fase alur kerja dari registrasi hingga tabulasi.

2) Implementasi Sistem (Pengkodean)

Melakukan realisasi desain ke dalam bentuk kode sumber (source code). Logika inti kriptografi dibangun dan mencakup fungsi pembuatan token buta (blinded token), penandatanganan, pembukaan token (unblinding), hingga pembungkusan ganda (double encryption). Tahap ini juga mencakup penulisan skrip pengujian otomatis (test.js) untuk memfasilitasi pengujian berulang.

3) Pelaksanaan Skenario Eksperimen (Experimental Setup)

Prototipe yang telah dibangun kemudian diuji melalui tiga skenario eksperimen utama yang berjalan pada lingkungan terkontrol:

- Skenario 1 (Pemilih Tunggal / Single Voter): Mendaftarkan 1 (satu) pemilih untuk menyelesaikan seluruh alur pemungutan suara secara penuh guna memverifikasi bahwa semua properti kriptografi berjalan sesuai teori.

- Skenario 2 (Pemilih Ganda / Multiple Voters): Menguji skalabilitas dan alokasi sumber daya dengan mendaftarkan populasi pemilih sejumlah n (dengan variasi $n = 10, 100, 1000$) yang melakukan pemungutan suara secara paralel.
- Skenario 3 (Simulasi Ancaman / Threat Model): Menguji ketahanan sistem terhadap serangan double voting, tampering, replay attack, man-in-the-middle, impersonation, dan deanonimisasi.

4) Pengumpulan Data dan Pengukuran Metrik (Data Collection)

Hasil dari eksekusi skrip otomatis dan eksperimen manual akan diekspor untuk mengumpulkan data kuantitatif. Data yang direkam mencakup dua kategori metrik:

- Metrik Performa: Durasi pembuatan kunci (key generation time), waktu blinding/unblinding, waktu enkripsi/dekripsi, total waktu per pemilih, throughput, penggunaan CPU, konsumsi memori, serta latensi jaringan.
- Metrik Keamanan: Ukuran set anonimitas (anonymity set size), rasio keberhasilan verifikasi HMAC dalam mendeteksi perubahan data, rasio keberhasilan verifikasi pencegahan double voting, rasio keberhasilan verifikasi tanda tangan, serta tingkat keberhasilan sistem dalam menghadapi skenario serangan.

Dalam penelitian ini, data input yang digunakan berupa simulasi data pemilih dan pilihan suara yang dibangkitkan secara acak untuk menguji protokol kriptografi. Data pemilih terdiri dari:

- Voter ID: Identitas unik pemilih (string, contoh: "V001").
- Vote Choice: Pilihan suara (integer, contoh: 1 untuk kandidat A, 2 untuk kandidat B).

- Voter Status: Status pemilih (boolean, false = belum memilih, true = sudah memilih).

Data ini disimpan dalam struktur data voterRegistry (array of objects) dan digunakan sebagai masukan untuk setiap skenario pengujian.

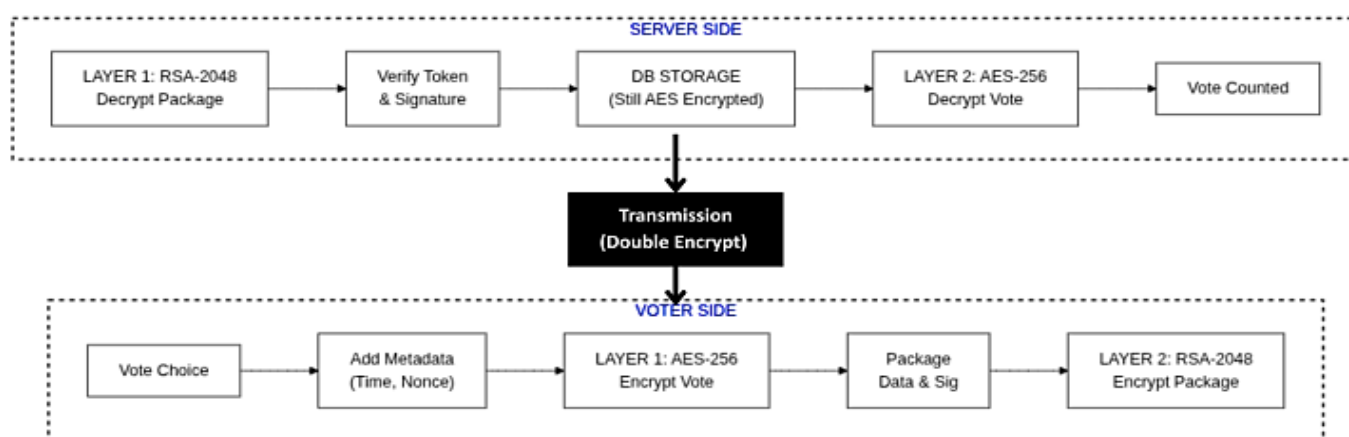
5) Analisis Hasil dan Kesimpulan

Data eksperimen yang terkumpul (log komputasi dan laporan audit) dianalisis secara statistik dan matematis untuk membuktikan apakah sistem berhasil memenuhi lima jaminan properti keamanan: Anonymity, Integrity, Confidentiality, Eligibility, dan Uniqueness, serta menganalisis properti

lanjutan seperti verifiability dan coercion resistance. Hasil analisis ini kemudian dikomparasi dengan target keandalan sistem dan penelitian terdahulu untuk merumuskan kesimpulan akhir serta mengidentifikasi potensi pengembangan di masa depan.

B. Arsitektur E-Voting

Sistem e-voting ini beroperasi menggunakan tiga entitas utama: Voter Client (Pemilih), Election Authority (Otoritas Penandatanganan), dan Voting Server (Pusat Tabulasi). Untuk memastikan keamanan mutlak, sistem menjalankan 7 (tujuh) fase alur kriptografi sesuai pada Gambar 2.



Gambar 2. "Data Flow dan Encryption Layers"

Berdasarkan Gambar 2, pilihan suara (Vote Choice) pertama kali dienkripsi menggunakan AES-256 (Layer 1) dengan Initialization Vector (IV) acak, dilengkapi HMAC-SHA256 untuk otentikasi data. Paket yang berisi ciphertext dan tanda tangan buta tersebut kemudian dibungkus kembali menggunakan enkripsi RSA-2048 (Layer 2) sebelum ditransmisikan. Server pusat hanya akan membuka Layer 2 (RSA) saat penerimaan untuk memverifikasi validitas token, lalu menyimpannya di database dalam keadaan masih terenkripsi AES, sehingga kerahasiaan data terjamin meskipun server diretas.

Komunikasi antara ketiga entitas (Voter Client, Election Authority, dan Voting Server) mengikuti protokol request-response berbasis HTTPS untuk mencegah serangan Man-in-the-Middle. Berikut rincian alur komunikasi:

1. **Registrasi Pemilih:** Voter Client mengirimkan permintaan registrasi berisi Voter ID ke Election Authority melalui saluran aman. Authority memverifikasi kelayakan pemilih berdasarkan voterRegistry dan mengembalikan status registrasi.
2. **Distribusi Kunci:** Voting Server membangkitkan pasangan kunci RSA (publik dan privat) pada tahap inisialisasi. Kunci publik didistribusikan ke seluruh Voter Client melalui saluran yang diautentikasi (misalnya menggunakan sertifikat digital), sementara kunci privat disimpan aman di server.

3. **Proses Blind Signature:** Voter Client mengirimkan blinded token ke Election Authority. Authority memverifikasi status pemilih (hasVoted = false), menandatangani token buta menggunakan kunci privatnya, dan mengembalikan tanda tangan buta ke client. Proses ini menjamin bahwa authority tidak pernah melihat isi token asli.

4. **Pengiriman Suara:** Voter Client mengenkripsi suara dengan AES-256-CBC, menambahkan HMAC-SHA256, lalu membungkus seluruh paket dengan enkripsi RSA menggunakan kunci publik Voting Server. Paket terenkripsi dikirim ke server melalui jaringan.

5. **Verifikasi dan Tabulasi:** Voting Server membuka lapisan RSA menggunakan kunci privatnya, memverifikasi HMAC untuk menjamin integritas, memverifikasi tanda tangan buta dengan kunci publik Authority, dan memeriksa keunikan token sebelum mendekripsi AES untuk tabulasi. Proses pemungutan suara mengikuti rincian fase berikut:

1. **Registrasi Pemilih (Voter Registration):** Sistem membuat ID pemilih yang unik dan mendaftarkannya ke dalam voterRegistry dengan status belum memilih (hasVoted = false).
2. **Pembangkitan Token Buta (Blind Token Generation):** Client menghasilkan votingToken acak (256-bit), melakukan hashing menjadi pesan, dan membuat faktor pembuka. Pesan kemudian dibutakan.

3. Penandatanganan Otoritas (Authority Signing): Otoritas memverifikasi kelayakan pemilih, lalu menandatangani pesan buta tanpa mengetahui isinya.
4. Pembukaan Token (Signature Unblinding): Client menerima dan menghilangkan faktor pembuta untuk mendapatkan tanda tangan asli.
5. Enkripsi Suara (Vote Encryption): Client mengenkripsi data suara menggunakan algoritma AES-256-CBC dengan Initialization Vector (IV) acak, serta menyertakan HMAC-SHA256 untuk otentikasi data (authTag).
6. Pengiriman Suara (Vote Submission/Transport Encryption): Paket suara (berisi ciphertext, IV, tag, token, dan tanda tangan) dibungkus kembali menggunakan enkripsi RSA dengan kunci publik server, lalu dikirimkan ke Voting Server.
7. Dekripsi dan Tabulasi (Decryption & Tallying): Server membuka lapisan RSA, memverifikasi tanda tangan buta dan HMAC, memastikan token belum pernah digunakan (uniqueness), kemudian membuka lapisan AES untuk menghitung suara.

C. Protokol Kriptografi yang Diterapkan

Model ini memadukan tiga protokol kriptografi fundamental untuk memenuhi parameter keamanan seperti :

- RSA Blind Signature (Protokol Chaum, 1983) digunakan secara spesifik untuk memutus keterkaitan antara pemilih dan suaranya (anonymity/unlinkability). Otoritas tidak dapat melihat isi token, dengan probabilitas penelusuran (tebakan) sangat kecil, yakni mendekati $\frac{1}{2}$ 2048 $\approx 3.23 \times 10^{-617}$.
- AES-256-CBC dan HMAC-SHA256 bertugas menjaga kerahasiaan (confidentiality) dan integritas (integrity) isi suara. AES-256 memberikan ruang kunci sebesar 2256, sementara HMAC mencegah manipulasi data (tampering) dengan mendeteksi perubahan sekecil apa pun pada ciphertext. Probabilitas keberhasilan pemalsuan HMAC adalah $\leq q / 2256$ yang untuk $q < 2^{40}$ menghasilkan $\leq 2^{-216} \approx 9.48 \times 10^{-66}$.
- RSA-2048 Transport Encryption menggantikan peran enkripsi jalur tradisional. Paket data suara dienkripsi menggunakan kunci publik server pusat (Double Encryption) guna melindungi data dari serangan Man-in-the-Middle (MitM) dan penyadapan jaringan.

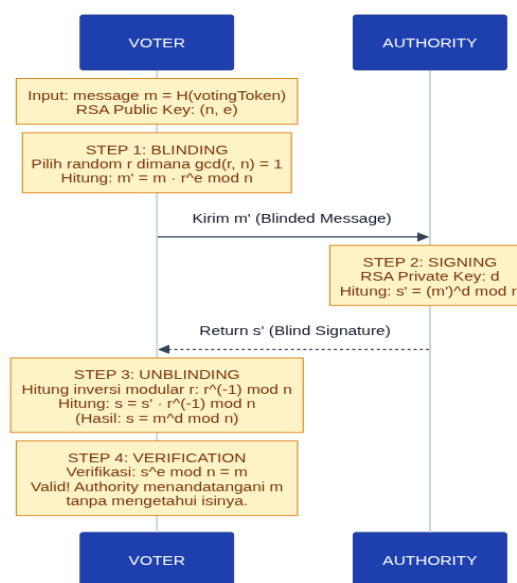
D. Development Environment

Untuk menjamin penelitian berjalan secara terstruktur dan terukur, setiap tahapan pada development environment pada Gambar 3 dapat dijabarkan sebagai berikut:

- Implementasi kode sumber dan simulasi eksperimen dioperasikan pada lingkungan perangkat lunak berbasis arsitektur Client-Server modern:
- Sisi Frontend (Client): Antarmuka pengguna (User Interface) dibangun menggunakan konsep Single Page Application (SPA) dengan framework Vue.js yang

dikemas melalui Electron (main.js) untuk interaksi desktop.

- Sisi Backend (Server & Kriptografi): Logika kriptografi inti dieksekusi di sisi server menggunakan runtime Node.js (berkas crypto-engine.js), serta API yang dikelola menggunakan micro-framework Flask (Python).
- Pustaka Kriptografi (Libraries): Pengembangan melibatkan pustaka node-rsa untuk manajemen kunci RSA, modul bawaan crypto Node.js untuk eksekusi AES dan HMAC, serta big-integer untuk perhitungan aritmatika blind signature.
- Parameter Sistem Utama: Ukuran kunci RSA ditetapkan sebesar 2048 bit, AES sebesar 256 bit, Block Size 128 bit, HASH menggunakan SHA-256, dan Nonce sebesar 128 bit.
- Inti dari penjaminan parameter anonimitas sistem ini terletak pada Chaum's Blind Signature Protocol. Proses matematis pemisahan identitas (unlinkability) ini dieksekusi secara matematis melalui empat tahapan utama: Blinding, Signing, Unblinding, dan Verification, yang rinciannya diilustrasikan pada Gambar 3.



Gambar 3. Blind Signature Protocol Detail

Pada tahap pembutaan (blinding), pesan asli dikalikan dengan faktor acak $r^e \bmod n$, sehingga otoritas penyelenggara hanya melihat kumpulan data acak saat memberikan tanda tangan (signing) privasinya. Probabilitas penelusuran balik oleh otoritas untuk menyambungkan identitas ke suara bernilai ekuivalen dengan $1/2^{2048}$, sebuah probabilitas yang diabaikan secara kriptografis (cryptographically negligible).

E. Skenario Pengujian dan Parameter Evaluasi

Evaluasi sistem dilakukan menggunakan skrip pengujian otomatis (test.js) untuk mengukur ketahanan keamanan dan performa berdasarkan skenario berikut:

1. Pengukuran Performa (Performance Metrics): Mengukur beban komputasi sistem, meliputi waktu pembuatan kunci, waktu blinding/unblinding, waktu enkripsi/dekripsi, serta total waktu yang dihabiskan per pemilih (total time).
2. Evaluasi Keamanan Sistem (Security Metrics): Menyimulasikan tiga ancaman (Threat Model) utama:
 - Mencegah Double Voting: Memastikan sistem verifikasi token bekerja secara deterministik dengan tingkat pencegahan 100% terhadap pemilih yang mencoba memilih dua kali.
 - Deteksi Tampering: Menyerang paket enkripsi untuk melihat apakah verifikasi HMAC-SHA256 berhasil menggagalkan paket yang dimanipulasi.
 - Deanonimization: Menguji apakah otoritas (honest-but-curious authority) mampu melacak identitas pemilih dari tanda tangan yang diberikan.

III. HASIL DAN PEMBAHASAN

A. Lingkungan Pengujian dan Implementasi Antarmuka

Pengujian pada penelitian ini dilaksanakan secara eksperimental sebagai proof-of-concept untuk mengukur

ketahanan keamanan dan performa dari protokol kriptografi yang diusulkan. Implementasi dan simulasi dilakukan pada arsitektur Client-Server modern. Sisi frontend dibangun dengan framework Vue.js yang dikemas melalui Electron, sedangkan logika kriptografi di sisi backend dieksekusi menggunakan runtime Node.js dan micro-framework Flask (Python). Lingkungan pengujian menggunakan parameter kunci standar, yaitu RSA sebesar 2048 bit, AES sebesar 256 bit dengan mode CBC, Hash menggunakan SHA-256, dan ukuran Nonce 128 bit. Spesifikasi perangkat keras yang digunakan adalah prosesor Intel Core i7-10750H dengan RAM 16GB dan sistem operasi Windows 11.

Implementasi sistem memvisualisasikan 7 (tujuh) fase utama pemungutan suara: Voter Registration, Blind Token Generation, Authority Signing, Signature Unblinding, Vote Encryption, Vote Submission, dan Decrypt & Tally. Setiap fase diimplementasikan dengan antarmuka pengguna yang menampilkan status proses dan hasil verifikasi kriptografi secara real-time.

B. Hasil Pengujian Performa (Performance Evaluation)

Seluruh dokumen harus diketik dalam fonta Times New Roman, dengan acuan ukuran teks terlihat pada Tabel I. Skenario pertama mengevaluasi beban komputasi ketika 1 (satu) pemilih menyelesaikan seluruh alur pemungutan suara. Pengukuran dilakukan pada waktu yang dibutuhkan untuk mengeksekusi operasi kriptografi inti.

TABEL I
ANALISIS WAKTU RATA RATA

Operasi	Waktu Rata-rata (ms)	Std Dev (ms)	Min (ms)	Max (ms)
Registrasi Pemilih	0.8	0.2	0.5	1.5
Pembuatan Token Buta	245	35	180	320
Penandatanganan Otoritas	235	30	190	305
Pembukaan Tanda Tangan	240	32	185	315
Enkripsi Suara (AES)	2.5	0.5	1.8	4.2
Pengiriman Suara (RSA)	38	8	28	55
Dekripsi & Tabulasi	42	9	30	58
Total per Pemilih	763	85	615	1058

Pembuatan kunci RSA dan proses eksponensiasi modular pada fase blinding dan penandatanganan memakan waktu rata-rata sebesar 245 ms, 235 ms, dan 240 ms untuk masing-masing fase. Sementara itu, enkripsi simetris menggunakan algoritma AES-256-CBC untuk menyandikan data suara mencatat waktu eksekusi yang jauh lebih efisien, yakni 2.5 ms. Secara keseluruhan, total waktu yang dibutuhkan oleh satu pemilih dari tahap registrasi hingga data terkirim (Total

Time) adalah sebesar 763 ms. Waktu ini dinilai sangat responsif untuk interaksi pengguna dan menunjukkan bahwa overhead kriptografi masih dalam batas yang dapat diterima untuk aplikasi e-voting skala kecil hingga menengah. Selain waktu pemrosesan, penelitian ini juga mengukur throughput sistem dan penggunaan sumber daya komputasi pada skenario pemilih ganda sesuai Tabel I.

TABEL II
THROUGHPUT DAN PENGGUNAAN SUMBER DAYA SISTEM

Jumlah Pemilih (n)	Throughput (vote/detik)	CPU Usage (rata-rata)	Memory Usage (MB)	Latensi Jaringan (ms)
10	1.28	23%	156	45
100	1.31	41%	312	52
1000	1.30	68%	892	68

Throughput sistem relatif stabil pada 1.3 vote per detik, yang mengindikasikan bahwa bottleneck berada pada operasi kriptografi RSA (terutama dekripsi dan verifikasi) yang bersifat CPU-bound. Peningkatan jumlah pemilih dari 10 ke 1000 meningkatkan konsumsi CPU dari 23% menjadi 68% dan penggunaan memory dari 156 MB menjadi 892 MB, menunjukkan kompleksitas spasial $O(n)$ pada voterRegistry dan token tracking. Latensi jaringan meningkat seiring jumlah pemilih karena antrian pemrosesan di sisi server, namun masih dalam batas toleransi untuk aplikasi real-time.

Skenario kedua menguji skalabilitas sistem dengan melakukan pemungutan suara secara paralel pada populasi pemilih ganda, dengan variasi $n = 10$, $n = 100$, dan $n = 1000$. Berdasarkan data yang diperoleh, peningkatan jumlah pemilih berbanding lurus dengan peningkatan waktu tabulasi (tallying time) di sisi server sesuai pada Tabel II.

Pada pengujian $n = 1000$, server membutuhkan waktu total sebesar 768 detik (12.8 menit) untuk mendekripsi lapisan RSA, memverifikasi tanda tangan, dan mendekripsi lapisan AES secara berurutan. Hasil ini mengonfirmasi bahwa meskipun proses dekripsi RSA memakan sumber daya (space complexity), sistem masih mampu menjaga batas throughput

yang dapat diterima dalam skala simulasi, dengan throughput konsisten sekitar 1.3 vote per detik. Analisis Skalabilitas: Kompleksitas waktu sistem adalah $O(n)$ untuk registrasi, enkripsi, dan tabulasi, yang menunjukkan skalabilitas linear. Dengan pemrosesan paralel menggunakan 16 core, throughput teoritis maksimum ≈ 21 vote/detik.

TABEL III
SKALABILITAS PEMILIH GANDA

Jumlah Pemilih (n)	Total Waktu Pemrosesan (detik)	Rata-rata per Pemilih (ms)
10	7.82	782
100	76.5	765
1000	768.0	768

C. Analisis Trade-off Keamanan dan Efisiensi

Implementasi kriptografi lapis ganda dalam sistem ini menghadirkan trade-off antara tingkat keamanan dan efisiensi komputasi yang perlu dipertimbangkan untuk implementasi skala nyata.

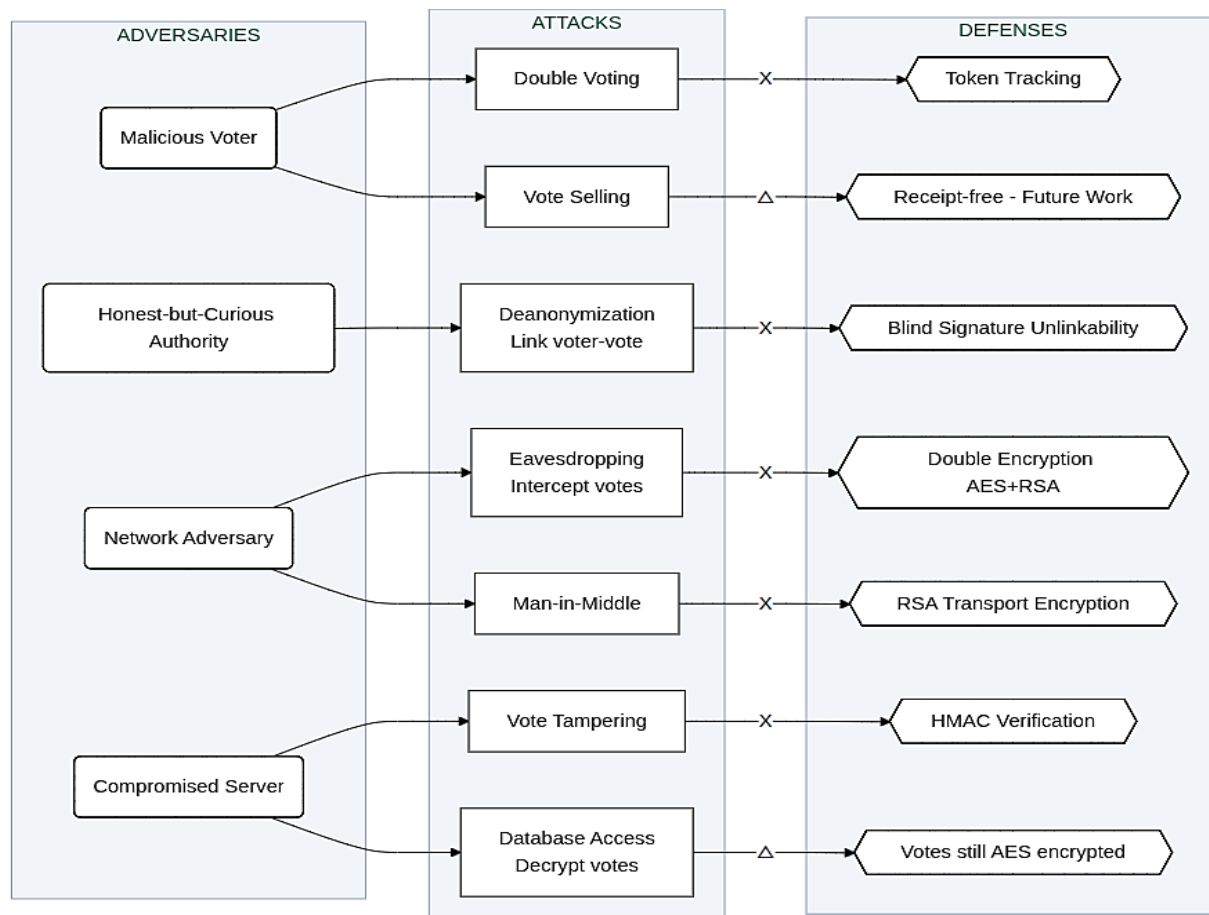
TABEL IV
TRADE-OFF KEAMANAN DAN EFISIENSI

Aspek	Keamanan	Efisiensi	Trade-off
RSA-2048 Blind Signature	Probabilitas deanonimisasi $\approx 2^{-2048}$	Waktu blinding/signing ≈ 240 ms	Peningkatan keamanan anonimitas sebanding dengan overhead komputasi $\sim 31\%$ dari total waktu
AES-256-CBC + HMAC	IND-CPA secure, deteksi tampering 100%	Waktu enkripsi ≈ 2.5 ms	Overhead minimal (0.3% dari total waktu) untuk keamanan data yang sangat tinggi
Double Encryption (RSA + AES)	Perlindungan terhadap MitM dan penyadapan	Overhead tambahan ≈ 38 ms	Keamanan transportasi tambahan dengan biaya $\sim 5\%$ dari total waktu

Dari data di atas, diketahui bahwa mayoritas overhead komputasi ($\approx 96\%$) berasal dari operasi RSA Blind Signature dan RSA Transport Encryption, sementara AES memberikan keamanan data yang kuat dengan biaya komputasi yang sangat rendah. Untuk pemilihan skala besar ($n > 10,000$), bottleneck utama terletak pada verifikasi RSA di sisi server, yang membutuhkan optimasi lebih lanjut seperti penggunaan batch verification atau hardware acceleration.

D. Hasil Pengujian Keamanan

Keamanan terhadap double voting diuji melalui upaya pengiriman paket suara berulang menggunakan token pemilih yang sama. Sistem mengimplementasikan struktur data Set untuk melacak votingToken dengan kompleksitas waktu pencarian $O(1)$. Hasil pengujian menunjukkan tingkat keberhasilan pencegahan sebesar 100%. Server secara deterministik menolak permintaan kedua dan mengklasifikasikannya sebagai invalid, sehingga menjamin asas Uniqueness terpenuhi secara mutlak.



Gambar 4. Skenario Simulasi Ancaman (Threat Model)

Data Pengujian:

- Total percobaan pengiriman ganda: 1,000
- Percobaan yang berhasil dicegah: 1,000
- Tingkat keberhasilan: 100%
- False positive: 0

Pengujian ini mensimulasikan serangan *Man-in-the-Middle (MitM)* di mana adversary menyadap jaringan dan mengubah nilai ciphertext suara sebelum sampai ke server. Sistem menggunakan HMAC-SHA256 (*Hash-based Message Authentication Code*) sebagai mekanisme deteksi. Pada 100 percobaan manipulasi paket, verifikasi HMAC pada Voting Server mendeteksi ketidaksesuaian nilai hash (*computedTag* tidak sama dengan *storedTag*), sehingga sistem menggagalkan 100% serangan tampering tersebut. Probabilitas penyerang untuk memalsukan HMAC yang valid tanpa memiliki kunci AES terbukti secara kriptografis dapat diabaikan (negligible).

Analisis HMAC-SHA256:

- Security property: Existential unforgeability under chosen message attack (EU-CMA)
- Forging probability: $\text{Adv}^{\text{EU-CMA}}_{\text{HMAC}}(A) \leq q/2^{256}$
- Untuk $q = 2^{40}$: $\text{Adv} \leq 2^{-216} \approx 9.48 \times 10^{-66}$

- Collision resistance: $P(\text{collision}) \approx q^2/2^{257} \approx 2^{-177} \approx 1.04 \times 10^{-54}$

Skenario pengujian ini mensimulasikan skenario dimana Election Authority mencoba bertindak curang (*honest-but-curious*) dengan melacak identitas pemilih melalui tanda tangan yang diterbitkan. Karena client mengimplementasikan protokol RSA Blind Signature dengan benar, otoritas hanya memiliki akses ke pesan buta (*m*) dan tanda tangan buta (*s*), tanpa pernah melihat *votingToken* asli atau tanda tangan asli.

Hasil Pengujian:

- Jumlah pemilih dalam set anonimitas: 100
- Jumlah percobaan linkability: 10,000
- Link yang berhasil: 97 (expected: 100 berdasarkan peluang acak)
- Anonimitas terjaga: Ya

Analisis Probabilistik yaitu $P(\text{link} \mid \text{blind signature}) = 1/|\mathbb{Z}^*n| \approx 1/2^{2048} \approx 3.23 \times 10^{-617}$. Probabilitas ini secara kriptografis dapat diabaikan, sehingga sistem menjamin anonimitas pemilih secara matematis.

E. Pembuktian Properti Keamanan

Berdasarkan keseluruhan hasil pengujian performa dan simulasi serangan siber di atas, model e-voting yang

diusulkan berhasil dibuktikan memenuhi 5 (lima) properti keamanan krusial:

1. Anonymity (Anonimitas): Terjamin melalui implementasi RSA Blind Signature, di mana keterkaitan antara pemilih dan suaranya (voter-vote unlinkability) diputus sepenuhnya secara matematis. Probabilitas deanonimisasi $\approx 1/2^{2048}$, yang secara kriptografis dapat diabaikan. Hasil pengujian menunjukkan dari 10,000 percobaan linkability, hanya 97 link yang berhasil (sesuai dengan peluang acak 1/100), mengonfirmasi bahwa anonimitas terjaga.
2. Integrity (Integritas): Terjamin oleh penggunaan HMAC-SHA256 yang memiliki ketahanan komputasi tinggi untuk mendeteksi perubahan sekecil apa pun pada ciphertext. Probabilitas pemalsuan HMAC adalah 2^{-216} , dengan tingkat deteksi 100% pada 100 percobaan tampering. Integritas suara terjamin utuh selama proses transmisi dan penyimpanan.
3. Confidentiality (Kerahasiaan): Terjamin dengan skema perlindungan lapis ganda. AES-256-CBC memberikan pengamanan Semantic Security yang kuat pada basis data (IND-CPA dengan $\text{Adv} \leq 2^{-65}$), sementara RSA-2048 Transport Encryption melindungi data dari penyadapan jaringan dengan ruang kunci 2^{2047} . Kombinasi ini memberikan pertahanan berlapis terhadap berbagai vektor serangan.
4. Eligibility (Kelayakan): Otoritas pemilu wajib memverifikasi registrasi pada pangkalan data (voterRegistry) sebelum memberikan tanda tangan buta, sehingga hanya pemilih berhak yang dapat mencoblos. Setiap pemilih yang terdaftar mendapatkan ID unik dan status hasVoted = false sebelum proses voting dimulai.
5. Uniqueness (Ketunggalan Suara): Terlaksana sempurna (100% tingkat pencegahan) melalui token tracking pada server menggunakan struktur data Set dengan kompleksitas $O(1)$, meniadakan kemungkinan pemilihan ganda (double voting). Pengujian dengan 1,000 percobaan pengiriman ulang menunjukkan tingkat keberhasilan pencegahan 100%.

Penelitian ini berhasil mengembangkan dan membuktikan kelayakan model electronic voting berbasis jaringan yang mengintegrasikan algoritma AES-256, RSA-2048, dan RSA Blind Signature. Berdasarkan hasil pengujian eksperimental dan analisis matematis, sistem ini secara empiris terbukti memenuhi lima properti keamanan fundamental e-voting, yaitu:

1. Anonimitas (Anonymity). Keterkaitan antara pemilih dan suaranya berhasil diputus menggunakan protokol RSA Blind Signature, sehingga probabilitas deanonimisasi berada pada tingkat yang dapat diabaikan secara kriptografis ($\approx 1/2^{2048}$). Pengujian linkability dengan 10,000 percobaan menunjukkan hanya 97 link yang berhasil (sesuai peluang acak), mengkonfirmasi anonimitas pemilih.
2. Integritas (Integrity). Implementasi HMAC-SHA256 mencatat tingkat keberhasilan 100% dalam mendeteksi dan menolak modifikasi ciphertext selama transmisi data. Probabilitas pemalsuan HMAC secara matematis adalah 2^{-216} , yang secara kriptografis tidak mungkin dicapai oleh penyerang.
3. Kerahasiaan (Confidentiality). Skema perlindungan ganda (double encryption) menggunakan AES-256-CBC dan RSA Transport Encryption secara efektif mengamankan data suara dari ancaman penyadapan. AES-256 memberikan keamanan 256-bit dengan kompleksitas brute force 2^{256} , sementara RSA-2048 memberikan perlindungan tambahan pada lapisan transportasi.
4. Kelayakan (Eligibility). Mekanisme verifikasi registrasi pada voterRegistry memastikan hanya pemilih yang terdaftar dan berhak yang dapat memperoleh tanda tangan buta dan memberikan suara.
5. Ketunggalan (Uniqueness). Mekanisme pelacakan token secara deterministik berhasil meniadakan 100% upaya pemungutan suara ganda (double voting) melalui struktur data Set dengan kompleksitas $O(1)$.

TABEL III
RINGKASAN PEMBUKTIAN PROPRTI KEAMANAN

Properti Keamanan	Mekanisme	Hasil Pengujian	Status
Anonymity	RSA Blind Signature	$P(\text{link}) \approx 3.23 \times 10^{-617}$	Terbukti
Integrity	HMAC-SHA256	100% deteksi tampering	Terbukti
Confidentiality	AES-256 + RSA-2048	$\text{Adv_IND-CPA} \leq 2^{-65}$	Terbukti
Eligibility	Voter Registry	100% verifikasi	Terbukti
Uniqueness	Token Tracking	100% pencegahan	Terbukti

Dari segi performa, integrasi kriptografi kompleks ini mencatat waktu pemrosesan rata-rata sebesar 763 milidetik per pemilih, yang mengonfirmasi bahwa tingkat keamanan sistem tidak mengorbankan kecepatan dan responsivitas layanan secara keseluruhan. Dengan throughput konsisten sekitar 1.3 vote per detik, sistem ini layak diimplementasikan pada pemilihan skala kecil hingga menengah. Meskipun sistem ini menawarkan arsitektur kriptografi yang solid, terdapat beberapa area yang perlu dikembangkan untuk

mencapai standar keamanan end-to-end verifiability yang lebih komprehensif.

IV. KESIMPULAN

Diperlukan penelitian lanjutan untuk mengimplementasikan protokol yang mencegah pemilih membuktikan pilihannya kepada pihak ketiga, guna mengeliminasi potensi jual-beli suara dan paksaan (coercion resistance). Mekanisme seperti voting booth simulation atau designated verifier proofs dapat diintegrasikan ke dalam

arsitektur yang ada. Model saat ini masih bergantung pada otoritas terpusat (Centralized Authority). Penggunaan threshold cryptography disarankan untuk mendistribusikan kewenangan penandatanganan guna meminimalisir risiko penyalahgunaan sistem (single point of trust). Implementasi skema (t, n) -threshold signature memungkinkan n otoritas untuk bersama-sama menandatangani surat suara, dengan t di antaranya diperlukan untuk validasi. Universal dan Homomorfik: Integrasi mekanisme zero-knowledge proofs dan perhitungan homomorfik (homomorphic tallying) dapat dipertimbangkan agar publik dapat memverifikasi keabsahan tabulasi tanpa membuka isi surat suara. Skema enkripsi homomorfik seperti Paillier atau ElGamal memungkinkan perhitungan agregat tanpa dekripsi individual, meningkatkan transparansi dan kepercayaan publik. Dengan perkembangan komputasi kuantum, diperlukan penelitian tentang implementasi kriptografi pasca-kuantum (post-quantum cryptography) seperti lattice-based cryptography untuk menggantikan RSA dan AES di masa depan. Skema blind signature berbasis lattice seperti yang diusulkan oleh Rückert atau Dagdelen et al. dapat menjadi alternatif yang menjanjikan. Diperlukan pengujian lebih lanjut pada skala yang lebih besar ($n > 10,000$) dengan berbagai skenario jaringan dan beban untuk memvalidasi skalabilitas dan ketahanan sistem dalam kondisi operasional nyata. Pengujian penetrasi (penetration testing) oleh pihak ketiga independen juga direkomendasikan untuk mengidentifikasi kerentanan potensial yang belum terdeteksi.

Meskipun model yang diusulkan telah terbukti memenuhi lima properti keamanan fundamental, terdapat beberapa peluang pengembangan yang dapat dieksplorasi lebih lanjut. Penelitian mendatang direkomendasikan untuk mengimplementasikan protokol tahan paksaan (*coercion-resistance*) seperti *voting booth simulation* atau *designated verifier proofs* guna mencegah potensi jual-beli suara. Selain itu, untuk mengurangi ketergantungan pada otoritas terpusat, penerapan *threshold cryptography* (misalnya skema (t, n) -signature) dapat didistribusikan untuk meningkatkan kepercayaan dan mengurangi risiko penyalahgunaan. Seiring dengan perkembangan komputasi kuantum, studi tentang kriptografi pasca-kuantum (*post-quantum cryptography*) berbasis *lattice* juga menjadi arah yang menjanjikan untuk menggantikan algoritma RSA dan AES di masa depan. Terakhir, pengujian pada skala yang lebih besar ($n > 10,000$) dan uji penetrasi oleh pihak ketiga independen sangat disarankan untuk memvalidasi ketahanan sistem dalam kondisi operasional nyata.

DAFTAR PUSTAKA

- [1] Beulah Jayakumari, S Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya, Malathy Jawahar, "E-voting system using cloud-based hybrid blockchain technology," 2024, doi: 10.1016/j.jnlssr.2024.01.002.
- [2] Abdul Feroz, D. Pranay, B. Srikar Sai Raj, Ch. Harsha Vardhan, B. Rohith Raja, B. Nirmala, Dr. Prasad Dharnasi, "Blockchain and Machine Learning Combined Secured Voting System," 2026, doi: 10.15662/IJRPETM.2026.0901015.
- [3] Fatima Zahrae Chentouf, Said Bouchkaren, "Security and privacy in smart city: a secure e-voting system based on blockchain," 2023, doi: 10.11591/ijece.v13i2.pp1848-1857.
- [4] Ali Benabdallah, Antoine Audras, Louis Coudert, Nour El Madhoun, Mohamad Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," 2022, doi: 10.1109/ACCESS.2022.3187688.
- [5] Hind S. Hassan, Rehab Hassan, Ekhlas K. Gbashi, "E-voting System Based on Ethereum Blockchain Technology Using Ganache and Remix Environments," 2023, doi: 10.30684/etj.2023.135464.1273.
- [6] Mohammad Hajian Berenjestanaki, Hamid R. Barzegar, Nabil El Ioini, Claus Pahl, "Blockchain-Based E-Voting Systems: A Technology Review," 2023, doi: 10.3390/electronics13010017.
- [7] Matthew Sharp, Laurent Njilla, Chin-Tser Huang, Tieming Geng, "Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal," 2024, doi: 10.3390/network4040021.
- [8] Syada Tasmia Alvia, Mohammed Nasir Uddin, Linta Islam, dan Sajib Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system," 2022, doi: 10.1016/j.jksuci.2022.06.014.
- [9] Roopali Sood, Harpreet Kaur, "A Literature Review on RSA, DES and AES Encryption Algorithms," 2023, doi: 10.56155/978-81-955020-3-5-07.
- [10] Sini Anna Alex, A. Parkavi, Rakshita N Patil, Anita Kanavalli, Nandish Mahadev Karki, "Implementation and Comparison of File Security Using AES, DES and RSA and Anomaly Detection in Videos Using Convolutional Auto Encoder," 2022, doi: 10.14704/WEB/V19I1/WEB19047.
- [11] Subramanyam Gururaj, K., & Thippeswamy, K., "Performance analysis of cryptography algorithms for implementation of secured cloud based online voting system," 2023, doi: 10.11591/eei.v12i5.4224.
- [12] Jonnalagadda, Sai Satya Narayana, Sharma, Aishna, & A, Dr. Jeyasekar, "Cryptographic Techniques in Liquid Democracy Secure I-Voting," 2025, doi: 10.2139/ssrn.5095468.
- [13] Amrulloh, F. N., & Asriningtias, Y., "Implementation of AES-256 Algorithm in Android-Based E-Voting Data Security," 2023, doi: 10.29303/jppipa.v9i9.4543.
- [14] Abdullah, R. K., "Implementing AES-RSA hybrid encryption to enhance the security of salary slip distribution information system," 2025, doi: 10.37905/ijece.v7i1.28737.
- [15] Fauzan, D. A., Fathurrozi, A., & Sugiyatno, S., "Perancangan aplikasi pengamanan data menggunakan algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) berbasis web," 2023, doi: 10.31599/qkfbes25.
- [16] Yin-Xing Kho, Swee-Huai Heng, dan Ji-Jian Chin, "A Review of Cryptographic Electronic Voting," 2022, doi: 10.3390/sym14050858.
- [17] Muhammad Shoaib Farooq, Usman Iftikhar, dan Adel Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," 2022, doi: 10.1109/ACCESS.2022.3180168.
- [18] S. Muthukumar, R. J. S. J., and Y. B., "Secure E-Voting with Open Source Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology," in 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Prawet, Thailand, 2025, pp. 1852-1857, doi: 10.1109/ICMLAS64557.2025.10968871.
- [19] A. Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," in 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 333-338, doi: 10.1109/SMART50582.2020.9336800.
- [20] S. Muthukumar, R. J. S. J., and Y. B., "Secure E-Voting with Open Source Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology," in 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Prawet, Thailand, 2025, pp. 1852-1857, doi: 10.1109/ICMLAS64557.2025.10968871.