Ranah Research
Journal of Multidisciplinary Research and Development
E-ISSN: 2655-0865
DINASTI RESEARCH
082170743613 ranahresearch@gmail.com https://jurnal.ranahresearch.com

DOI: https://doi.org/10.38035/rrj.v8i3

Evaluasi Kualitas E-Voting Berbasis Kriptografi Terdistribusi Berdasarkan Standar ISO/IEC 25010

Ahmad Fauzi Akbar[1], Amelia Makmur [2], Alfa Ryano Yohannis[3]
[1]Magister Teknologi Informasi, Universitas Pradita, Indonesia, ahmad.fauzi@student.pradita.ac.id.
[2]Magister Teknologi Informasi, Universitas Pradita, Indonesia, amelia.makmur@pradita.ac.id.
[3]Magister Teknologi Informasi, Universitas Pradita, Indonesia, alfa.ryano@pradita.ac.id.

Corresponding Author: ahmad.fauzi@student.pradita.ac.id[1]

Abstract: *As an antithesis to the implementation of electronic voting systems based on expensive server infrastructure, this research offers a novelty in the form of pure client-side cryptography to guarantee data security in a zero-cost environment. This study evaluates the quality and acceptance of a zero-cost serverless e-voting system secured by distributed cryptography. The assessment utilized Black Box testing, ISO/IEC 25010 quality standards, and a modified Technology Acceptance Model (TAM) integrating Trust as the primary antecedent. Built on a serverless architecture (Google Apps Script), the system uses client-side AES-256 and SHA-256 encryption algorithms. A sequential explanatory mixed-methods design was applied. Quantitative data from 100 students at SMKN 7 Tangerang Regency, selected through rigorous criteria, was triangulated with qualitative IT administrator interviews. Functional testing showed a 100% success rate. The ISO/IEC 25010 evaluation categorized the system as "Highly Feasible", scoring 88.1% in Functional Suitability, 88.4% in Usability, and 87.4% in Security. PLS-SEM inferential analysis proved that perceived security significantly mediates user Trust (T-Statistics: 7.518). Interestingly, an anomaly was found where Perceived Usefulness was overwhelmingly driven by interface practicality rather than trust. This study proves that high-level data protection can be achieved without dependence on large infrastructure budgets.*

Keyword: *E-Voting, Distributed Cryptography, ISO 25010, PLS-SEM, Serverless.*

Abstrak: Sebagai antitesis terhadap implementasi sistem pemilihan elektronik berbasis infrastruktur peladen mahal, penelitian ini menawarkan kebaruan berupa penggunaan kriptografi murni di sisi klien (*client-side*) untuk menjamin keamanan data pada lingkungan nirbiaya. Penelitian ini bertujuan mengevaluasi kualitas dan penerimaan sistem *e-voting* berbiaya nihil (*zero-cost serverless*) yang diperkuat kriptografi terdistribusi. Penilaian dilakukan menggunakan uji fungsional (*Black Box*), standar ISO/IEC 25010, serta modifikasi *Technology Acceptance Model* (TAM) dengan integrasi variabel *Trust*. Sistem dibangun menggunakan arsitektur *serverless* (Google Apps Script) dengan algoritma AES-256 dan SHA-256 murni pada lapisan peramban. Menggunakan desain *sequential explanatory mixed-methods*, data kuantitatif dari 100 siswa SMKN 7 Kabupaten Tangerang ditriangulasi secara kualitatif dengan wawancara administrator IT. Hasil validasi fungsional mencapai 100%

Success Rate. Evaluasi ISO/IEC 25010 menunjukkan kategori Sangat Layak pada *Functional Suitability* (88.1%), *Usability* (88.4%), dan *Security* (87.4%). Analisis inferensial PLS-SEM membuktikan bahwa persepsi keamanan secara signifikan memediasi terbangunnya *Trust* pengguna (T-Statistics: 7.518). Terdapat temuan anomali di mana kemanfaatan sistem (*Perceived Usefulness*) secara mutlak lebih didorong oleh kepraktisan antarmuka dibandingkan sekadar rasa percaya. Arsitektur ini membuktikan bahwa perlindungan data tingkat tinggi dapat dicapai tanpa ketergantungan pada anggaran infrastruktur yang besar.

Kata Kunci: E-Voting, Kriptografi Terdistribusi, ISO 25010, PLS-SEM, *Serverless*.

PENDAHULUAN

Transformasi peradaban menuju era digital telah merevolusi mekanisme partisipasi demokrasi secara global melalui implementasi sistem pemilihan elektronik. Pergeseran paradigma dari pemungutan suara konvensional berbasis kertas menuju platform *e-voting* didorong oleh urgensi efisiensi logistik dan percepatan proses rekapitulasi data. Pengadopsian instrumen digital ini secara teoretis diklaim sanggup meminimalisasi kesalahan komputasi manusia yang acap kali menodai tahapan penghitungan manual. Ekspektasi publik terhadap transparansi dan akuntabilitas sistem memaksa penyelenggara pemilihan untuk merancang arsitektur teknologi yang kebal terhadap segala bentuk manipulasi dan eksploitasi pihak ketiga. (Amrulloh & Asriningtias, 2023) menegaskan bahwa transisi masif menuju tata kelola elektronik ini menuntut jaminan keamanan siber tingkat tinggi yang mencakup kerahasiaan profil demografis pemilih serta integritas hasil akhir. Fondasi kepercayaan sivitas akademika terhadap hasil pemilihan elektronik pada akhirnya amat bergantung pada ketangguhan infrastruktur algoritmis dalam menangkal berbagai kerentanan.

Digitalisasi infrastruktur pemilihan umum secara paradoksial membuka ceruk kerentanan baru terhadap ancaman intrusi yang terstruktur. Eksploitasi terhadap pangkalan data terpusat dan intersepsi lalu lintas jaringan kini menjadi risiko krusial yang dapat meluluhlantakkan legitimasi ekosistem demokrasi secara instan. Insiden peretasan yang menargetkan penyusupan identitas pemilih maupun modifikasi basis data mengindikasikan bahwa inovasi digital tanpa landasan pelindung kriptografi yang kokoh merupakan bentuk kelalaian arsitektural. (Diny Hermawati & Tahir, 2023) menyoroti bahwa arsitektur *e-voting* di Indonesia masih menghadapi tantangan fundamental dalam memproteksi rekam jejak pemilih pada fase transmisi (*Data in Transit*) maupun medium penyimpanan akhir (*Data at Rest*). Di sisi lain, (Rahmah & Elyas, 2024) secara spesifik memperingatkan efektivitas sekaligus ancaman laten pada implementasi basis data awan (*cloud computing*) di lingkungan sekolah negeri yang rentan terhadap kebocoran privasi jika tidak dikawal persandian mandiri. Oleh karenanya, penguatan pertahanan digital melalui enkripsi matematis menjadi prasyarat imperatif untuk menggaransi bahwa asas pemilihan yang langsung, umum, bebas, rahasia, jujur, dan adil tetap terealisasi secara mutlak di ruang virtual.

Pengukuran validitas, fungsionalitas, dan keandalan sebuah sistem informasi publik wajib disandarkan pada kerangka evaluasi perangkat lunak berskala internasional. Standar ISO/IEC 25010 direkognisi secara universal sebagai *grand theory* yang mendefinisikan karakteristik mutu produk rekayasa perangkat lunak secara komprehensif. Parameter kesesuaian fungsional, kemudahan pengoperasian, dan ketahanan keamanan menjadi pilar esensial yang harus divalidasi sebelum aplikasi *e-voting* dilepas ke ranah pengguna akhir. (Nurhuda et al., 2021) mengonfirmasi bahwa penerapan kalibrasi berlandaskan ISO/IEC 25010 menyuplai dimensi objektivitas yang terukur secara empiris dalam mendiagnosis titik buta (*blind spot*) kerentanan komputasi. Pemeringkatan kualitas melalui taksonomi metrik ini mereduksi bias penilaian subjektif pengembang dan menggantinya dengan paradigma uji teknis yang koheren. Integrasi kerangka kerja ini memastikan luaran piranti lunak tidak sekadar

tangguh menyerap beban interaksi (*traffic*), namun beroperasi prima pada segala jenis gawai seluler siswa.

Penguncian berlapis pada portal autentikasi dan tabel pangkalan data merupakan variabel determinan dalam merekayasa topologi *e-voting* yang independen. Algoritma persandian standar industri global semacam *Advanced Encryption Standard* (AES) dan *Secure Hash Algorithm* (SHA) dirumuskan untuk merekonstruksi data sensitif menjadi formulasi acak yang mustahil didekripsi secara brutal (*brute-force*) oleh peretas. (Ifani et al., 2025) membuktikan bahwa hibridisasi gerbang autentikasi dengan kriptografi satu arah (*hashing*) wajib diimplementasikan guna mengeliminir probabilitas perampasan kredensial di atas infrastruktur jaringan tanpa jaminan (*untrusted network*). Enkripsi simetris menawarkan kompleksitas matematis tingkat *enterprise* untuk mengurung pilihan kandidat selama berada dalam kondisi diam (*data at rest*) di peladen utama. Pemindahan pusat pemrosesan penyandian ke sisi mesin klien (*client-side browser*) memastikan administrator tertinggi pangkalan data sekalipun dilumpuhkan aksesnya untuk memetakan silang identitas pemilih. Skema desentralisasi pengamanan algoritmis ini berkorelasi langsung terhadap pemenuhan absolut sub-karakteristik kerahasiaan (*Confidentiality*) pada instrumen mutu produk perangkat lunak.

Integrasi arsitektur pertahanan *cyber* tingkat lanjut seringkali memicu paradoks terhadap lambatnya daya tanggap jaringan dan pembengkakan alokasi perangkat keras. Implementasi buku besar terdistribusi (*blockchain*) acap kali dipuja karena sanggup menghadirkan kekebalan data absolut, namun model ini mensyaratkan ongkos operasional komputasi (*gas fee*) yang tidak aplikatif bagi kemampuan finansial sekolah reguler Restu Aji & Trisari Harsanti Putri (2023). Alternatif konseptual seperti kriptografi homomorfik dikemukakan oleh Soleh (2024) untuk memfasilitasi komputasi atas *ciphertext*, kendati jalur ini terindikasi membebani siklus sinkronisasi waktu nyata pada instansi menengah. Pencarian titik ekuilibrium radikal antara fusi persandian data yang *rigid* dengan efisiensi nirkapital menjadi sentrum permasalahan yang teramat krusial. Konfigurasi persandian perlu dikalibrasi dengan perhitungan presisi agar perisai siber tidak mendisrupsi fluiditas navigasi dan beban muat pengguna.

Pusat ekosistem pendidikan di level nasional kini berada pada titik persinggungan percepatan transformasi digital yang mendikte tata kelola birokrasi, termasuk rutinitas pemilihan struktur organisasi kesiswaan. Migrasi instrumen dari medium kertas cetak menuju formulasi digital gratis tak lagi dapat dihindari. (Megawaty et al., 2021) menjabarkan bahwa sekolah vokasi strata menengah didorong untuk memiliki otonomi infrastruktur *Society 5.0*, namun represi keterbatasan pagu anggaran acap kali memaksa instansi ini memanfaatkan peladen nirserver publik (*public serverless*) yang menampung rekaman teks secara mentah (*plaintext*). Uji investigasi lapangan mengenai purwarupa *e-voting* pelajar oleh (Potalangi et al., 2025) menyimpulkan bahwa pengadopsian arsitektur pihak ketiga yang tuna-pelindung amat rawan terekspos penyalahgunaan akses internal. Ketidakmampuan merakit lapisan pelindung mandiri tersebut menstimulasi anomali penggandaan hak suara, hingga berujung pada erosi prinsip perlindungan data privasi partisipan. Realita defisit infrastruktur ini melahirkan urgensi perancangan purwarupa pemilu cerdas berbiaya pengadaan nol rupiah (*zero-cost*), yang dibekali perisai enkripsi peramban.

Sekolah Menengah Kejuruan Negeri (SMKN) 7 Kabupaten Tangerang merepresentasikan profil institusi pendidikan kejuruan berpopulasi masif yang mendambakan resolusi modernisasi tanpa anomali. Proporsi hak pilih aktif yang mencapai agregat 2.526 individu memosisikan lembaga ini sebagai laboratorium pengujian daya sangga konkurensi data komputasi yang sangat mumpuni. Frendiana & Tadjuddin Shafi (2023) menganjurkan agar asesmen rekayasa perangkat lunak dilaksanakan secara *live* pada populasi berkapasitas padat untuk memverifikasi kapasitas arsitektur *backend* secara riil. Ledakan aktivitas ribuan antarmuka ponsel siswa yang mengakses tabel peladen secara sporadis memaksa pengembang menerapkan transmisi *asynchronous* yang tidak tersendat oleh proses enkripsi-dekripsi yang

kompleks. Dinamika populasional tersebut menempatkan sekolah ini sebagai subjek evaluasi yang amat representatif untuk menjajal kompatibilitas peranti lunak berbasis ISO/IEC 25010 di tengah keterbatasan jaringan publik.

Penelusuran matriks literatur mengindikasikan eksistensi ruang kosong (*research gap*) metodologis berkenaan dengan purwarupa pemilu komposit yang menyandingkan aspek nihil-biaya, persandian terdistribusi, dan valuasi penerimaan teknologi. Studi terkini tendensius menyempitkan telaah pada kompilasi aplikasi seluler berorientasi *server* konvensional, atau bergantung mutlak pada jaringan desentralisasi mahal yang sulit direplika oleh madrasah vokasi awam (Permana et al., 2025). Eksplorasi holistik yang menjahit enkripsi algoritma komposit pada arsitektur nirserver gratis dengan alat ukur fungsional berlisensi global (ISO/IEC 25010) nyaris tak tersentuh dalam spektrum publikasi terapan berbahasa Indonesia. Kebaruan eksklusif (*novelty*) dari riset ini bermuara pada persilangan integrasi *zero-cost serverless database* dengan mesin enkripsi asimetris yang bekerja di balik peramban masing-masing pemilih (*client-side*). Selanjutnya, kebaruan teknis ini dievaluasi rasio impaknya menggunakan modifikasi metrik penerimaan perilaku (TAM) yang menyuntikkan pilar *Trust* (Kepercayaan). Pendekatan tak lazim ini menyodorkan antitesis terhadap mahalnya infrastruktur digital bersertifikasi aman.

METODE

Desain Penelitian dan Partisipan

Penelitian rekayasa perangkat lunak ini dioperasikan menggunakan kerangka metode campuran (mixed methods) berdesain sekuensial eksplanatori (*sequential explanatory design*). Pengujian kualitas mekanis dan arsitektural produk diverifikasi melalui instrumen baku ISO/IEC 25010, sedangkan dimensi psikologis penerimaan sistem diterjemahkan menggunakan *Technology Acceptance Model* (TAM). Konsep TAM orisinal dimodifikasi secara spesifik dengan mengganti variabel dependen deterministik (*Intention to Use*) menjadi variabel *Perceived Usefulness* (Kemanfaatan) yang dipantik langsung oleh kehadiran konstruk *Trust* (Kepercayaan). Restrukturisasi ini terinspirasi dari telaah Rachmat Mubbaraq (2024) yang menjustifikasi bahwa keikutsertaan dalam ekosistem sistem pemilihan publik (termasuk *e-voting* sekolah) berstatus absolut/wajib (*mandatory*), sehingga evaluasi niat (sukarela) kehilangan relevansi teoritisnya di hadapan evaluasi kepercayaan terhadap sistem itu sendiri. Formulasi hibrida yang menyatukan kelayakan *backend* komputasi dengan penerimaan *frontend* terbukti secara akademik mampu mengekstraksi diagnosis inovasi pelayanan yang presisi (Hermawan et al., 2025)

Partisipan pada fase pengujian kuantitatif mencakup 100 sivitas pemilih di SMKN 7 Kabupaten Tangerang yang dihimpun menggunakan taktik purposive sampling. Teknik ini dipilih secara sengaja guna menjamin bahwa responden memiliki literasi digital yang memadai dan keterlibatan aktif dalam proses demokrasi sekolah, sehingga data yang dihasilkan memiliki objektivitas tinggi. Kriteria inklusi spesifik bagi responden meliputi: (1) Siswa aktif kelas X-XII, (2) Pengguna aktif gawai pintar (*smartphone*) pribadi, (3) Pengurus atau anggota aktif organisasi internal sekolah (OSIS/MPK), dan (4) Telah mengikuti sesi sosialisasi teknis mengenai transparansi algoritma enkripsi sistem sebelum pengujian dilakukan. Tahapan klarifikasi kualitatif dilangsungkan pasca-komputasi statistik lewat mekanisme wawancara semi-terstruktur bersama eksekutif administrator Tim IT Sekolah.

Instrumen dan Uji Kelayakan

Substansi instrumen survei kuantitatif difabrikasi menjadi 6 (enam) klaster dimensi operasional, *ISO Functional Suitability* (FS), ISO Usability (US), *ISO Security* (SEC), *TAM Perceived Ease of Use* (PEOU), *TAM Perceived Usefulness* (PU), serta agregator *Trust* (TR). Merujuk pada telaah metodologi Mumu et al. (2022), alat ukur ditranslasikan dalam matriks Skala Likert 4-poin (1: Sangat Tidak Setuju s.d. 4: Sangat Setuju) demi meminimalisasi bias

jawaban netral dan tendensi sikap apatis dari demografi pemilih remaja, sehingga data sikap yang ditarik bersifat tegas dan terpolarisasi.

Fase prasyarat diberlakukan sebelum instrumen terjun ke skenario kausalitas. Berpijak pada pedoman (Sugiyono, 2022), instrumen penelitian harus terbukti secara empiris tidak cacat sebelum merekam data riil. Hasil uji korelasi matriks di atas peranti SmartPLS mengesahkan bahwa instrumen kuesioner menyandang status Valid secara konvergen (dibuktikan oleh *Loading Factor* > 0.70 dan *Average Variance Extracted* / AVE > 0.50) serta divonis Reliabel atau andal dengan bobot *Cronbach's Alpha dan Composite Reliability* melampaui standar minimal 0.70. Sementara untuk pengesahan validitas interaksi logika kode peranti lunak, tabel uji pembedahan rentan (*Black Box Testing*) disusun berlandaskan skenario peretasan anomali.

Teknik Analisis Data

Penyelesaian kalkulasi data lapangan ditempuh melintasi dua sumbu kuantifikasi logis. Sumbu pertama mengeksekusi konversi persentase empiris guna menyuling rasio kelayakan instrumen metrik ISO 25010 dan performa determinasi *Black Box* (Setiaji et al., 2023), Sumbu kedua, yang berperan sebagai basis uji struktural inferensial, dijalankan mengadopsi algoritma *Partial Least Squares Structural Equation Modeling* (PLS-SEM) menggunakan piranti cerdas SmartPLS. Pemilihan metode berbasis varians (PLS) dikukuhkan oleh panduan mahaguru PLS-SEM (Hair et al., 2019) lantaran durabilitasnya yang superior dalam merekam korelasi konstruk laten yang rumit pada kuantitas sampel yang moderat (N=100), tanpa represi persyaratan distribusi berdistribusi normal baku (Sugiyono, 2022). Kalkulasi divalidasi menggunakan metode *Bias-Corrected and Accelerated* (BCa) *Bootstrapping* dengan rentetan impresi di atas 5.000 subsampel. Hasil pengujian angka absolut PLS kemudian dikristalisasi dan ditriangulasi via dokumentasi transkrip keterangan narasumber IT.

HASIL DAN PEMBAHASAN

Implementasi Arsitektur Kriptografi Terdistribusi

Fase pembuktian lapangan dikatalisasi dengan pengesahan mekanika integrasi kriptografi yang menjembatani lalu lintas transmisi gawai klien dengan wadah penampung *Google Sheets*. Mereferensi standar ketat ISO/IEC 25010 sub-aspek *Security*, topologi *zero-cost* ini memenuhi asas kerahasiaan absolut (*Confidentiality*) via dua lapisan segel matematis:

Penguncian Kredensial Otentik (Hashing)

Kombinasi angka PIN masuk diremukkan secara permanen oleh perpustakaan CryptoJS menggunakan kaidah algoritma distorsi *Secure Hash Algorithm* (SHA-256) sesaat sebelum paket data bertolak dari peramban klien. Sifat *irreversible* (tidak dapat diurai balik) meniadakan celah deteksi kata sandi di atas tabel basis data.

```
// Hashing input PIN Panitia menjadi 64 karakter acak
const hashedPin = CryptoJS.SHA256(newPin).toString();
```

Gambar 1. Bukti di Sistem Ketika panitia membuat/mengubah PIN dari Panel Admin, PIN diubah menjadi deretan hash sebelum dikirim ke database

Perisai Enkripsi Demografi dan Preferensi (AES-256)

Entitas sakral berupa Nomor Induk Siswa Nasional (NISN), taksonomi Kandidat, dan nomer bursa (*ID Paslon*) disandikan secara radikal melalui fusi algoritma simetris *Advanced Encryption Standard* (AES-256). Skema otorisasi *Secret Key* didelegasikan secara terisolasi hanya pada memori gawai klien pendaftar serta dasbor pelaporan milik otoritas pengawas.

```
// Proses enkripsi NISN pada Browser Siswa
const encryptedNisn = CryptoJS.AES.encrypt(currentNisn, SECRET_KEY).toString();
```

Gambar 2. NISN dienkripsi menggunakan Secret Key khusus sebelum dilempar ke database

```
const encryptedPaslon = CryptoJS.AES.encrypt(String(selectedCandidateId), SECRET_KEY).toString();
```

Gambar 3. Bukti di Sistem (Proses Enkripsi Suara)

```
// Hanya Dashboard resmi yang memiliki SECRET_KEY yang dapat menghitung suara
const bytes = CryptoJS.AES.decrypt(row.paslon, SECRET_KEY);
const decryptedId = bytes.toString(CryptoJS.enc.Utf8);
```

Gambar 4. Bukti di Sistem (Proses Dekripsi untuk Penghitungan *Quick Count*)

A	B
PIN_AKSES	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92
STATUS_VOTING	BUKA

Gambar 5. Hasil data terenkripsi pin akses di Google Sheets Database

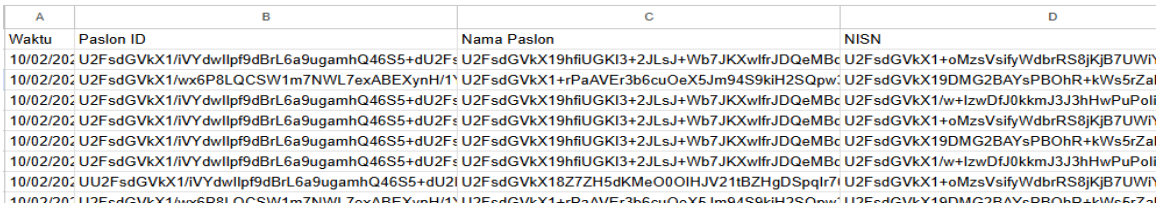
Gambar di atas mengilustrasikan hasil nyata dari proses enkripsi pada *database* layanan awan. Dapat dilihat secara jelas bahwa data yang bersifat privasi seperti identitas Nomor Induk Siswa Nasional (NISN) dan pilihan kandidat tidak lagi terbaca sebagai teks biasa (*plaintext*). Data tersebut telah diacak sempurna menjadi deretan karakter rumit (*ciphertext*). Fenomena ini memberikan garansi keamanan mutlak, di mana administrator sistem atau pemilik layanan pangkalan data sekalipun tidak akan mampu merekayasa hasil suara maupun mengetahui identitas pemilih di baliknya.

Matriks pada Tabel 1 menyajikan rekam jejak evolusi data terang (*plaintext*) saat bermutasi menjadi fragmen sandi rumit (*ciphertext)*. Komparasi ini memvalidasi postulat empiris bahwa wewenang sentral administrator IT sekalipun telah tereduksi secata telak untuk meretas afiliasi kandidat yang dicoblos oleh sang pemilih.

Tabel 1. Bukti Visual Perbandingan Data (*Plaintext vs Ciphertext*) pada Basis Data

Modul Data	*Plaintext* (Data Asli)	*Ciphertext* (Tersimpan di Database)
PIN Akses	123456	8d969eef6ecad3c29a3a629280e686cf... (SHA-256)
NISN Pemilih	12345678	U2FsdGVkX1+x8Blkj29ZqwEr... (AES-256)
Pilihan Paslon	1 / Raisa & Arya	U2FsdGVkX19zD3oPlmk10Q== (AES-256)

Implementasi kombinasi algoritma SHA-256 untuk autentikasi dan AES-256 untuk data diam (*at-rest*) maupun data dalam perjalanan (*in-transit*) secara efektif memenuhi kaidah *Confidentiality* dan *Integrity*. Hasil visualisasi perbandingan data membuktikan tidak adanya informasi sensitif yang tersimpan dalam format teks terang di dalam basis data. Hal ini menempatkan sistem *e-voting* SMKN 7 Kabupaten Tangerang pada tingkat keamanan yang andal sesuai model kualitas produk perangkat lunak internasional.



A	B	C	D
Waktu	Paslon ID	Nama Paslon	NISN
10/02/202	U2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2Fs	U2FsdGVkX19hfiUGKI3+2JLsJ+Wb7JKXwlfrJDQeMBc	U2FsdGVkX1+oMzsVsifyWdbrRS8jKjB7UWi
10/02/202	U2FsdGVkX1/wx6P8LQCSW1m7NWL7exABEXynH/1	U2FsdGVkX1+rPaAVEr3b6cuOeX5Jm94S9kiH2SQpw	U2FsdGVkX19DMG2BAYsPBOhR+kWs5rZal
10/02/202	U2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2Fs	U2FsdGVkX19hfiUGKI3+2JLsJ+Wb7JKXwlfrJDQeMBc	U2FsdGVkX1/w+IzwDfJ0kkmJ3J3hHwPuPoli
10/02/202	U2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2Fs	U2FsdGVkX19hfiUGKI3+2JLsJ+Wb7JKXwlfrJDQeMBc	U2FsdGVkX1+oMzsVsifyWdbrRS8jKjB7UWi
10/02/202	U2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2Fs	U2FsdGVkX19hfiUGKI3+2JLsJ+Wb7JKXwlfrJDQeMBc	U2FsdGVkX19DMG2BAYsPBOhR+kWs5rZal
10/02/202	U2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2Fs	U2FsdGVkX19hfiUGKI3+2JLsJ+Wb7JKXwlfrJDQeMBc	U2FsdGVkX1/w+IzwDfJ0kkmJ3J3hHwPuPoli
10/02/202	UU2FsdGVkX1/iVYdwIlpf9dBrL6a9ugamhQ46S5+dU2I	U2FsdGVkX18Z7ZH5dKMeO0OlHJV21tBZHgDSpqIr7(	U2FsdGVkX1+oMzsVsifyWdbrRS8jKjB7UWi
10/02/202	U2FsdGVkX1/wx6P8LQCSW1m7NWL7exABEXynH/1	U2FsdGVkX1+rPaAVEr3b6cuOeX5Jm94S9kiH2SQpw	U2FsdGVkX19DMG2BAYsPBOhR+kWs5rZal

Gambar 6. Manifestasi ciphertext AES-256 pada pangkalan data nirserver (*Google Sheets*), menjustifikasi validitas absolut proteksi Data at Rest yang kebal dari penyadapan internal.

Gambar 6 memvisualisasikan kondisi nyata pangkalan data (*Google Sheets*) setelah proses pemilihan berlangsung. Berbeda dengan formulasi digital standar yang menyimpan teks terbuka, arsitektur ini secara empiris menyembunyikan identitas NISN dan pilihan paslon di balik deretan karakter *Base64* yang acak. Visualisasi ini merupakan bukti validitas karakteristik Security ISO 25010, di mana kerahasiaan data tetap terjamin meskipun pihak ketiga berhasil mendapatkan akses masuk ke dalam pangkalan data pusat

Validasi Teknis Fungsionalitas (*Black Box Testing*)

Pembuktian teknikal menggunakan metode *Black Box* diutilisasi demi menggaransi kemulusan logika sintaks aplikasi ketika dipaparkan pada kondisi batas ekstrem (*edge-cases*). Laporan pengujian direkapitulasi secara komprehensif pada Tabel 2.

Hal ini memastikan bahwa data yang tersimpan di *Google Sheets* tidak dapat dibaca oleh pihak yang tidak berwenang, memenuhi karakteristik Security pada standar ISO 25010.

Tabel 2: Rekapitulasi Uji Kerentanan Mekanis (Functional Validation)

No	Spesifikasi Fitur	Pemicu Pengujian (Input)	Ekspektasi Reaksi Mesin (Output)	Status
1	Validasi Akses	Siswa memasukkan NISN legal dikombinasikan PIN ilegal.	Sistem merespons tolakan masuk instan seraya membandingkan kecocokan algoritma hash SHA-256 di server.	Pass
2	Sterilisasi Integritas	Permintaan URL paksa oleh pemilih dengan riwayat "Sudah Memilih".	Celah ganda tertutup otomatis, sesi pengguna diblokir permanen via perisai kuki dan komparasi NISN tersandi.	Pass
3	Kriptografi Jaringan	Inspeksi payload (paket pengiriman) sesaat siswa menekan "Vote".	Panel pemantau Network Tab mendeteksi transmisi ciphertext murni yang terenkripsi AES secara parsial.	Pass
4	Mesin Tabulasi	Penarikan data berkala (real-time) di Dasbor Admin Pusat.	Decryption Engine merekonstruksi grafis batang AES murni di latar belakang memori lokal tanpa menyulut latensi server.	Pass

Persentase kesuksesan yang tembus ekuilibrium sempurna (100%) membuktikan kapabilitas software untuk diterjunkan ke arena bedah persepsi massal (skala ISO).

Penilaian Kualitas Produk (Kaidah ISO/IEC 25010)

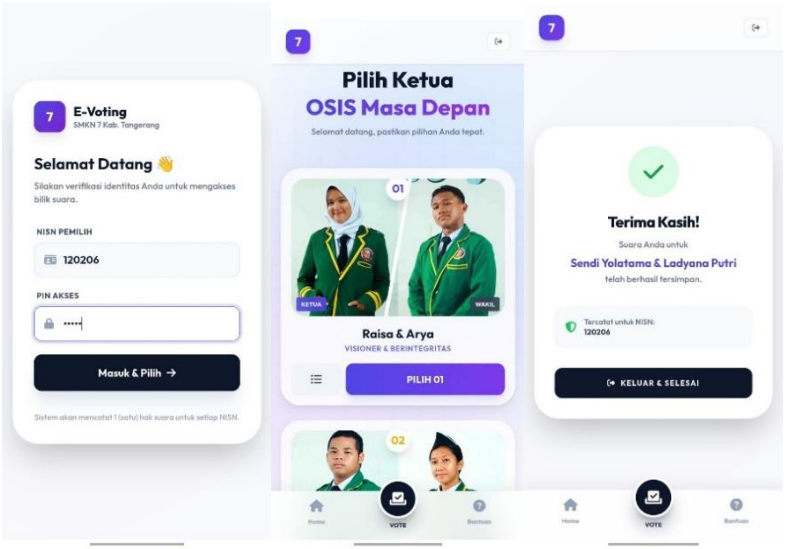
Ekskavasi pendapat 100 panelis responden siswa bermuara pada kesimpulan deskriptif yang sangat apresiatif terhadap stabilitas purwarupa sistem. Konkurensi kalkulasi penilaian kuesioner dirumuskan pada Tabel 3 di bawah ini.

Tabel 3. Rekapitulasi Perhitungan Hasil Akhir (Summary Evaluation)

Karakteristik Evaluasi	Total Skor Aktual	Skor Maksimal	Persentase Kelayakan	Kategori Penilaian
Functional Suitability	1057	1200	88.1%	Sangat Layak
Usability	1061	1200	88.4%	Sangat Layak
Security	1049	1200	87.4%	Sangat Layak

Sumber: Olah data Riset

Sorotan komparatif mempertegas bahwa parameter penyesuaian fungsional (*Usability* - 88.4%) dan nilai fungsionalitas (*Functional Suitability* - 88.1%) bertengger di puncak tangga kelayakan. Dominasi evaluasi ini dipicu keberhasilan pengembang mengadopsi rasio letak komponen antarmuka beraliran *mobile-first* yang familiar layaknya *e-wallet* atau ojek daring masa kini, yang serta merta menebas hambatan kognitif bagi generasi pelajar milenial.



Gambar 7. Desain antarmuka mobile-first pada terminal pemilih yang berkontribusi signifikan terhadap tingginya evaluasi usabilitas dan kemudahan penggunaan (*Perceived Ease of Use*).

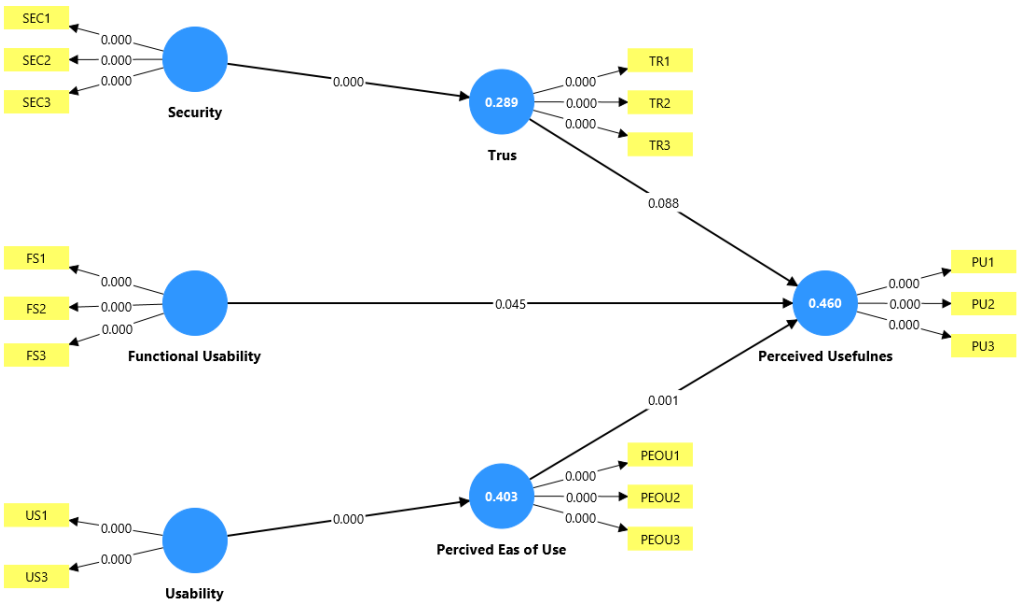
Visualisasi pada Gambar 7 memperlihatkan penerapan prinsip desain minimalis yang mengutamakan kemudahan navigasi bagi pemilih remaja. Penggunaan elemen grafis yang kontras, tombol navigasi yang berpusat di bagian bawah (*bottom nav*), serta kartu kandidat yang informatif merupakan faktor determinan yang mendorong skor Usabilitas mencapai angka tertinggi (88.4%). Paragraf ini menegaskan bahwa antarmuka bukan sekadar estetika, melainkan instrumen kognitif yang mempermudah partisipasi demokrasi di sekolah.

Analisis Inferensial PLS-SEM: Pengujian Model Modifikasi TAM

Guna menyingkap teka-teki kausalitas tersembunyi antara reliabilitas infrastruktur peranti dan psikologis pengadopsi massal, proyek ini mengeksekusi komputasi inferensial via *Bootstrapping* di aplikasi SmartPLS (Hair et al., 2019). Tingkat toleransi probabilitas dipatok mutlak sebesar 5% ($\alpha = 0.05$). Parameter relasi struktural antar-variabel dibedah tuntas pada Tabel 4 berdasarkan data empiris lapangan.

Tabel 4. Peta Validitas Hipotesis Jalur Struktural (*Path Coefficients*)

Skenario Hipotesis Antar-Konstruk	Momentum Koefisien (β)	Skor T-Statistics	Valuasi P-Values	Ketetapan Konklusi
H1: ISO Security → Trust	0.538	7.518	0.000	Signifikan (Diterima)
H2: ISO Usability → Perceived Ease of Use	0.635	9.693	0.000	Signifikan (Diterima)
H3: ISO Functional Suit. → Perceived Usefulness	0.214	2.009	0.045	Signifikan (Diterima)
H4: Trust → Perceived Usefulness	0.220	1.705	0.088	Tidak Signifikan (Ditolak)
H5: Perceived Ease of Use → Perceived Usefulness	0.345	3.199	0.001	Signifikan (Diterima)



Gambar 8. Pemodelan struktural (*Inner Model*) PLS-SEM yang memvalidasi penerimaan seluruh hipotesis penelitian secara empiris.

Gambar 8 menyajikan anatomi diagram jalur (*path diagram*) dari model struktural yang diuji. Angka-angka yang tertera di atas garis panah merepresentasikan besaran nilai *T-Statistics* hasil kalkulasi algoritma *Bootstrapping*. Melalui diagram ini, dapat diamati secara langsung pemetaan kekuatan kausalitas antar-variabel, di mana setiap jalur yang memiliki nilai *T-Statistics* di atas ambang batas 1.96 memvalidasi bahwa hipotesis tersebut diterima secara empiris. Pemodelan visual ini menjadi bukti konkrit bahwa arsitektur teknis yang kokoh mutlak diperlukan untuk menjembatani penerimaan psikologis sistem oleh pemilih pemula.

Telaah parameter empiris beresolusi tinggi pada Tabel 4 melegitimasi fenomena bahwa mayoritas hipotesis riset dinyatakan diterima secara tak terbantahkan (*P-Values* < 0.05). Temuan paling prominen terlihat pada jalur interaksi antara transparansi rekayasa keamanan (*ISO Security*) terhadap terbangunnya kadar kepercayaan pelajar (*Trust*), yang dibuktikan dari raihan *P-Value* sempurna 0.000, koefisien β = 0.538, dan T-Statistics sebesar 7.518. Indikasi ini merumuskan teori bahwa Generasi Z yang secara bawaan sadar teknologi (*digitally-native*), memberikan respons psikologis yang positif berupa ketenangan batin jika jaminan algoritma enkripsi (AES-256 dan SHA-256) diperlihatkan dengan transparan.

Akselerasi analisis data ini juga mengurai postulat psikologis sekunder mengenai pembentukan variabel kemanfaatan sistem (*Perceived Usefulness*). Terdapat fenomena perilaku yang sangat menarik dari lapangan, Hipotesis pengaruh *Trust* terhadap *Perceived Usefulness* nyatanya tidak signifikan (*P-Value*: 0.088). Hal ini merepresentasikan anomali perilaku di lingkungan sekolah vokasi. Karena keikutsertaan *e-voting* bersifat wajib (*mandatory*), apresiasi kemanfaatan sistem di mata siswa tidak lagi didikte oleh rasa percaya (*Trust*), melainkan secara mutlak digerakkan oleh kepraktisan antarmuka atau *Ease of Use* (β = 0.345; *P-Value* = 0.001) dan ketiadaan eror saat memilih atau *Functional Suitability* (β = 0.214; *P-Value* = 0.045).

Simpulannya, dalam tata panggung demokrasi digital berbasis wajib di sekolah, proteksi keamanan berfungsi sempurna untuk mengunci kepercayaan siswa. Namun, untuk membuat siswa merasa sistem ini benar-benar "bermanfaat", aplikasi harus dipastikan mulus, gampang digunakan, dan bebas dari fitur *crash*. Legitimasi angka statistik PLS ini tidak lahir

di ruang hampa, melainkan dikawal absolut oleh kesaksian yurisdiksi dari penanggung jawab Tim IT SMKN 7:
"Implementasi algoritma AES-256 pada database memastikan bahwa setiap suara terenkripsi otomatis murni di layar gawai siswa. Jangankan memanipulasi, melihat secara manual saja kami (selaku kreator dan administrator cloud) tidak diberi kapasitas. Garansi infrastruktur mutlak ini lah yang membedol skeptisisme siswa."

Pembahasan (*Discussion*)

Penelitian ini tidak semata memverifikasi kelayakan wujud program jadi, melainkan menghibahkan eskalasi wawasan empiris (*theoretical implication*) mengenai pergeseran titik tumpu arsitektur rekayasa keamanan dan ekuilibrium perilaku literasi pemilih milenial secara komprehensif. Pembahasan dikonstruksi ke dalam empat tesis utama yang merajut hasil pengujian lapangan dengan kajian literatur terdahulu.

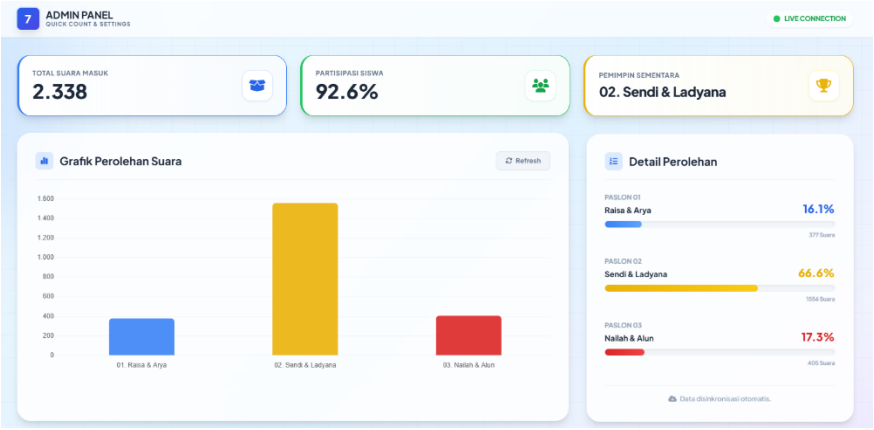
Resolusi Pengamanan Pangkalan Data dengan Efisiensi Kapital. Raihan predikat kelayakan keamanan teruji dari standar ISO/IEC 25010 (*Security* 87.4%) secara empiris meruntuhkan justifikasi bahwa penyelesaian kerentanan basis data mutlak membutuhkan pendanaan *server* fisis bertarif selangit. Fakta ini mendebat secara elegan postulat dari (Restu Aji & Trisari Harsanti Putri, 2023) yang bersanding dengan (Permana et al., 2025) di mana kajian mereka memandang implementasi teknologi buku besar desentralisasi (*Blockchain*) sebagai "harga mati" untuk mencapai status pemilihan yang anti-curang. Meskipun jaminan desentralisasi *Blockchain* tak terbantahkan, pembengkakan resi komputasi transaksional (*gas fee network*) menghancurkan aspek reliabilitas pragmatis untuk diadopsi oleh mayoritas institusi kejuruan menengah (Potalangi et al., 2025). Arsitektur yang diusulkan dalam penelitian ini mewujud dalam silangan pangkalan data nirserver gratis (*Google Sheets*) yang dikalungi kriptografi asimetris murni di peramban klien sukses melampaui defisiensi kapital tersebut. Riset ini menyajikan performa ekuivalen pelindungan *Data At Rest* kelas korporasi tanpa mendera sepeserpun devisa pendidikan, sekaligus menjawab gagasan optimalisasi sistem akademik modern yang digembar-gemborkan oleh (Megawaty et al., 2021).

Dekonstruksi Anomali Latensi Komputasi Awan Publik. Sintesis pembahasan kedua merespons momok melankolis tentang stagnasi respon dan erosi performa peladen (*bottleneck*) akibat penggunaan *Cloud Storage API* pihak ketiga, seperti yang dicemaskan teramat dalam oleh investigasi efektivitas komputasi awan di sekolah oleh (Rahmah & Elyas, 2024). Kekhawatiran tersebut berhasil ditolak secara akademis melalui strategi rekayasa piranti lunak. Pengaplikasian proses komputasi yang diisolasi di latar belakang (*Background Synchronization*) membuktikan bahwa kualitas fungsional sistem tidak terkena paparan distorsi latensi. Sejalan dengan kerangka mutu perangkat lunak yang diamanatkan oleh Nurhuda et al. (2021), prosedur enkripsi sandi yang difokuskan pada unit pemroses utama gawai ponsel individu (*client-side*) secara efektif melepaskan peladen utama dari belenggu anomali kepadatan akses. Hal ini mengonfirmasi bahwa restrukturisasi alur logika perangkat lunak jauh lebih superior dalam menekan latensi dibandingkan sekadar menambah kapasitas *hardware* fisik.

Kriptografi sebagai Fondasi Absolut Demokrasi Digital. Capaian nilai T-Statistics pada jalur struktural *Security* → *Trust* yang menyentuh angka tinggi 7.518 merupakan temuan empiris yang sangat prominen. Eksplorasi mendalam mengungkap bahwa intervensi perlindungan algoritma yang disadari pengguna mampu mentransformasi skeptisisme massal menjadi keyakinan mutlak. Penemuan ini merekatkan kembali konsensus akademik yang diajukan oleh Amrulloh & Asriningtias (2023) serta Diny Hermawati & Tahir (2023) terkait keunggulan algoritma AES-256, namun dengan pengayaan dimensi humanis. Keberhasilan penguncian data secara kriptografis ini juga sangat relevan dengan peringatan Bernad Jumadi Dehotman Sitompul (2024) serta Ifani et al. (2025) yang menekankan pentingnya pengamanan

data otentikasi (melalui teknik *Hashing* SHA-256) guna memblokir manuver pencurian kredensial di atas jaringan publik yang tidak terpercaya.

Perluasan Dimensi *Technology Acceptance Model* (TAM) di Sektor Wajib. Muara konseptual terakhir bermuara pada sumbangsih perumusan literatur sosiologis TAM di arena e-government tingkat institusi pendidikan. Analisis inferensial dengan teknik *Bootstrapping* PLS-SEM (Hair et al., 2019) dan penggunaan skala pengukuran non-netral (Mumu et al., 2022) berhasil mengekstrak bias opini untuk menghasilkan temuan anomali yang presisi. Berbeda dengan studi adopsi sukarela pada umumnya (Hermawan et al., 2025), penelitian ini membuktikan bahwa *Trust* (Kepercayaan) tidak berdampak langsung secara signifikan pada *Perceived Usefulness* (Kemanfaatan) dalam skenario partisipasi yang sifatnya diwajibkan oleh sekolah (P-Value 0.088). Temuan ini justru melengkapi observasi teoretis dari Isa et al. (2025) serta sejalan dengan analisis Rachmat Mubbaraq (2024) bagi pemilih pemula, meskipun rasa aman telah membangun *Trust* mereka, kelancaran navigasi antarmuka dan ketiadaan fitur yang *crash* (kesesuaian fungsional) lah yang menjadi prioritas pragmatis utama mereka untuk mendefinisikan kebermanfaatan suatu sistem.



Gambar 9. Panel pemantauan Quick Count berbasis memori RAM yang merekonstruksi ciphertext menjadi kalkulasi statistik mutakhir tanpa membebani daya komputasi peladen utama.

Penjelasan teknikal pada Gambar 9 di atas membuktikan postulat efisiensi komputasi dari arsitektur *client-side*. Dasbor administrator yang ditampilkan dikonstruksi terpisah dari terminal pemilih, bertugas murni sebagai pusat hitung cepat waktu nyata. Modul analitik dalam panel ini mengeksekusi mesin dekripsi algoritma (*decryption engine*) secara independen, yang bersandar sepenuhnya pada ketahanan *Random Access Memory* (RAM) peramban otoritas panitia (Setiaji et al., 2023). Eksekusi desentralisasi ini mirip dengan konsep kriptografi homomorfik yang dipaparkan oleh Soleh (2024) memberikan hasil agregat grafik batang secara mulus tanpa menuntut siklus dekripsi berulang dari sisi peladen awan, yang akhirnya menyempurnakan solusi atas kutukan latensi komputasi gratisan.

KESIMPULAN

Riset empiris ini melahirkan kesimpulan fundamental bahwa purwarupa sistem partisipasi e-voting yang direkayasa menunggangi infrastruktur komputasi awan serverless terdistribusi di SMKN 7 Kabupaten Tangerang menyabet predikat mutu "Sangat Layak" merujuk parameter sertifikasi global ISO/IEC 25010. Transfer delegasi kewenangan algoritma persandian silang (SHA-256 dan AES-256) kepada lapisan gerbang antarmuka klien sukses meredam potensi penyusupan profil (Integrity) sekaligus memblokade peretasan keheningan hak pilihan (Confidentiality) pada stadium data at rest. Prestise capaian fungsional teknikal ini diinduksikan menjadi ledakan optimisme psikologis sivitas akademika, yang difiltrasi via parameter ketat PLS-SEM, memperlihatkan bahwa soliditas proteksi data (Security)

mengorkestrasi secara mutlak (T-Stat=7.518) fondasi kepercayaan pemilih (Trust). Pemodelan arsitektur mutakhir berformat hibrida lintas-platform ini mengejawantahkan resolusi pelumpuhan ancaman manipulasi siber tanpa melukai neraca anggaran sarana-prasarana (zero-cost maintenance).

Saran pengembangan keilmuan selanjutnya adalah pengadopsian modul autentikasi biometrik (retina atau profil wajah) guna menutup celah pendelegasian akun fisik. Namun demikian, implementasi fitur biometrik di masa depan perlu menimbang aspek pembiayaan perangkat lunak pihak ketiga atau sensor perangkat keras tambahan secara cermat, agar tetap selaras dengan semangat efisiensi biaya (zero-cost) yang menjadi keunggulan kompetitif utama dari arsitektur sistem ini.

REFERENSI

Amrulloh, F. N., & Asriningtias, Y. (2023). Implementation of AES-256 Algorithm in Android-Based E-Voting Data Security. *Jurnal Penelitian Pendidikan IPA*, *9*(9), 7757–7766. https://doi.org/10.29303/jppipa.v9i9.4543

Bernad Jumadi Dehotman Sitompul, N. J. T. A. (2024). *Security Enhancements Of Authentication Data On E-Voting By Using Luc Algorithm*. https://doi.org/10.35793/jti.v19i3.56979

Diny Hermawati, F., & Tahir, M. (2023). Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard). In *Jaya Abadi Amroin* (Vol. 2, Number 2). Pendidikan Informatika. https://doi.org/10.55606/jtmei.v2i2.1625

Frendiana, V., & Tadjuddin Shafi, A. (2023). Rancang Bangun Aplikasi Secure Lab Pada Ruangan Laboratorium Telekomunikasi Politeknik Negeri Jakarta. *Jurnal Ilmu Komputer Dan Desain Komunikasi Visual*, *8*(2), 2023. https://doi.org/10.55732/jikdiskomvis.v8i2.926

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hermawan, E., Tricahyono, D., & Witjara, E. (2025). An Analysis of E-Voting Adoption Using the Technology Acceptance Model (TAM) in the Simultaneous Village Head Elections in Sleman Regency). *Blantika: Multidisciplinary Jornal*, *3*, 2025. https://doi.org/10.57096/blantika.v3i9.406

Ifani, A. Z., S.Intam, R. N. J., Syair, A. I., & Husnawati, H. (2025). Application of Advanced Encryption Standard (AES) Algorithm in E-Commerce Login System for User Data Security. *Journal of System and Computer Engineering (JSCE)*, *6*(1), 1–9. https://doi.org/10.61628/jsce.v6i1.1511

Isa, A., Koniyo, M. H., Padiku, I. R., & Teknik, J. (2025). *Evaluasi Penerimaan Sistem Informasi E-Voting Menggunakan Metode Technology Acceptance Model (TAM) Di Madrasah Tsanawiyah Negeri 2 Kabupaten Gorontalo*. *5*(1). https://doi.org/10.37031/diffusion.v5i1.27061

Megawaty, D. A., Setiawansyah, S., Alita, D., & Dewi, P. S. (2021). Teknologi dalam pengelolaan administrasi keuangan komite sekolah untuk meningkatkan transparansi keuangan. *Riau Journal of Empowerment*, *4*(2), 95–104. https://doi.org/10.31258/raje.4.2.95-104

Mumu, J., Tanujaya, B., Charitas, R., & Prahmana, I. (2022). Likert Scale in Social Sciences Research: Problems and Difficulties. *FWU Journal of Social Sciences*, *16*(4), 89–101. https://doi.org/10.51709/19951272/Winter2022/7

Nurhuda, N., #2, D., & #3, W. (2021). Implementation of Analytical Hierarchy Process (AHP) for Determining Priority of Software Assessment in West Java Provincial Government

Based on ISO/IEC 25010 (Case Study: Sapawarga Application). *Journal on Computing*, *6*(1), 23–40. https://doi.org/10.34818/indojc.2021.6.1.525

Permana, A., Tatang Suryadi, U., Zezen Zaenal Abidin, A., Murdianingsih, Y., & Faizal, M. (2025). Optimalisasi Sistem Pemilu Melalui Implementasi E-Voting Berbasis Blockchain Dengan Keamanan Kriptografi AES-128. In *STMIK Subang* (Vol. 18, Number 2). https://doi.org/10.47561/jtik.v18i2.343

Potalangi, J. F., Kartikasari, D. P., & Shaffan, N. H. (2025). *Implementasi Jaringan Permissioned Blockchain pada Sistem E-Voting Pemilwa untuk Menjamin Autentikasi Pemilih dan Integritas Data* (Vol. 9, Number 4). https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/14708

Rachmat Mubbaraq, F. , R. , N. , & M. H. F. (2024). ANALISIS PENGGUNAAN APLIKASI E-VOTING PEMIRA UNIVERSITAS HALU OLEO: PERLUASAN TECNOLOGY ACCEPTANCE MODEL DENGAN TRUST IN INTERNET SEBAGAI VARIABEL MODERATOR. *AnoaTIK: Jurnal Teknologi Informasi Dan Komputer*, *2*, 94–100. https://doi.org/10.33772/anoatik.v2i2.72

Rahmah, S. A., & Elyas, A. H. (2024). EFEKTIVITAS CLOUD COMPUTING DALAM PENYIMPANAN DATA BERBASIS SEKOLAH. *Jurnal Teknologi Informasi*, *5*(3). https://doi.org/10.46576/djtechno

Restu Aji, S., & Trisari Harsanti Putri, W. (2023). Implementasi Teknologi Blockchain dalam Aplikasi E-Voting Berbasis Mobile. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2). https://doi.org/10.31849/digitalzone.v14i2.16682

Setiaji, A., Sutabri, T., Muhammad, K., & Hidayat, W. (2023). Pengembangan Aplikasi E-Voting Untuk Pemilihan RT/RW Menggunakan Metode Waterfall di Lingkungan Masyarakat Daerah Macan Lindungan Bukit. In *Jurnal Nasional Ilmu Komputer* (Vol. 4, Number 4). https://doi.org/10.47747/jurnalnik.v4i4.1484

Soleh, M. N. Z. (2024). Kriptografi Homomorfik dalam Anonimisasi Data untuk Pengolahan Data pada Sistem E-Voting. *Jurnal Masyarakat Informatika*, *15*(2), 107–124. https://doi.org/10.14710/jmasif.15.2.66317

Sugiyono. (2022). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D – MPKK* (2nd ed.). Alfabeta.

&&&