Implementasi Cyber Security untuk Menjaga Integritas Data dalam Sistem Pemilu Digital

Disusun oleh:

KELOMPOK E

Varen Aditya Swastama	103012330442
Fidhela Ghaisani Shabrina	103012300320
Muhammad Ihsan Naufal	103012300288
Muhammad Raihan Hadi Pamungkas	103012300222
Adi Bintang Syahputra	103012300499

FAKULTAS INFORMATIKA

S1 INFORMATIKA

TELKOM UNIVERSITY BANDUNG

2025

DAFTAR ISI

BAB I

PENDAHULUAN

1. Latar Belakang

Perkembangan digitalisasi layanan publik serta pemilu yang semakin bergantung pada sistem digital membuat isu integritas data sebagai salah satu kunci untuk mencapai tujuan pembangunan berkelanjutan (SDG) di Indonesia, khususnya SDG 16 tentang Perdamaian, Keadilan, dan Institusi yang Kuat. SDG 16 menekankan pentingnya membangun institusi yang transparan, akuntabel, dan bebas dari korupsi untuk terciptanya masyarakat yang damai dan inklusif. Integritas data adalah fondasi bagi institusi modern saat pengambilan keputusan, pelayanan publik, dan penanggulangan masalah. Pada tingkat pemerintahan dan lembaga publik, kerusakan atau manipulasi data dapat melemahkan proses demokrasi, mengurangi kepercayaan publik, dan merusak akuntabilitas suatu negara terhadap warga negaranya. Oleh karena itu, diperlukan perlindungan integritas data yang baik untuk menjaga demokrasi dan menciptakan tata kelola pemerintahan yang baik. Kualitas dari desain langkah-langkah keamanan suatu institusi menjadi faktor krusial dalam penerapan demokrasi di institusi tersebut. Mulai dari penilaian risiko, enkripsi data, autentikasi, praktik pengkodean aman, audit berkala, hingga rencana respons insiden.

(SUGESTI REVISI LATAR BELAKANG)

Digitalisasi dalam penyelenggaraan pemilu membawa kemajuan, tetapi juga membuka celah ancaman terhadap integritas data. Keamanan siber menjadi hal krusial untuk menjaga keaslian hasil, mencegah manipulasi, dan mempertahankan kepercayaan publik terhadap sistem pemilu digital.

Pemilu yang rentan terhadap peretasan, sabotase data, atau gangguan sistem dapat merusak legitimasi demokrasi. Oleh karena itu, diperlukan strategi keamanan siber yang kuat, mulai dari enkripsi, autentikasi, audit, hingga regulasi yang mendukung. Upaya ini sejalan dengan SDG 16 yang mendorong institusi yang transparan, akuntabel, dan bebas dari korupsi.

2. Rumusan Masalah

1. Apa tantangan utama dalam implementasi cyber security dalam sistem pemilu digital?
2. Bagaimana implementasi keamanan data yang efektif untuk mencegah manipulasi pada pemilu digital?
3. Bagaimana regulasi pemerintahan dapat memperkuat integritas data dan kepercayaan publik terhadap pemilu digital?

3. Tujuan

1. Menganalisis tantangan utama dalam implementasi keamanan siber pada sistem pemilu digital.
2. Merumuskan strategi implementasi keamanan data yang efektif untuk mencegah manipulasi pada pemilu digital.
3. Mengidentifikasi peran regulasi pemerintah dalam memperkuat integritas data dan kepercayaan publik terhadap pemilu digital.

4. Manfaat

1. Menjadi landasan dalam identifikasi dan pemahaman tantangan utama keamanan siber pada pemilu digital agar dapat diantisipasi sejak dini.
2. Memberikan gambaran strategi pengamanan data yang efektif untuk mencegah manipulasi dan menjaga keaslian hasil pemilu digital.
3. Menjadi landasan bagi penguatan regulasi pemerintah dalam membangun integritas data serta meningkatkan kepercayaan publik terhadap sistem pemilu digital.

BAB II

KAJIAN LITERATUR

1. Pemilu Digital, Integritas Data, dan Keamanan Siber

Transformasi digital dalam proses pemilu membuat tahapan kritis seperti pendaftaran pemilih, pencoblosan, perhitungan, hingga publikasi hasil kini semakin bergantung pada infrastruktur elektronik. Hal ini membuka dua sisi yaitu peningkatan efisiensi dan transparansi, tetapi juga meningkatkan risiko manipulasi data, gangguan layanan, dan juga serangan siber yang dapat merusak hasil pemilu. Upaya menjaga integritas data itu menjadi kunci untuk mempertahankan kepercayaan publik serta akuntabilitas institusi demokrasi, yang selaras dengan tujuan SDG 16 tentang institusi yang transparan, akuntabel, dan bebas korupsi.

Keamanan siber tidak hanya dipahami sebagai perlindungan sistem TI dari serangan teknis, tetapi juga sebagai mekanisme pertahanan demokrasi. Ketika data suara pemilu bisa dimanipulasi atau sistem pemilu digital diretas, konsekuensinya bukan sekedar kerugian teknis, melainkan hilangnya legitimasi politik dan juga berkurangnya kepercayaan publik terhadap proses pemilu. Karena itu, banyak riset yang bergerak ke arah arsitektur pemilu digital yang memiliki properti seperti *confidentiality* (kerahasiaan), *integrity*, auditabilitas, dan transparansi dan keterpercayaan publik.

2. Blockchain sebagai Mekanisme Keamanan dan Integritas dalam Sistem E-Voting

Banyak literatur yang memilih blockchain sebagai kandidat utama untuk mengatasi masalah integritas data dan transparansi dalam sistem pemilu digital. Blockchain dipandang menarik karena memiliki sifat terdesentralisasi, immutable, dan transparan. Untuk artikel jurnal ini kami akan menggunakan dua artikel sebagai fondasi kajian literatur yang membahas blockchain sebagai solusi untuk keamanan, integritas, auditabilitas, dan kepercayaan publik dalam e-voting, dari dua artikel ini memiliki sudut pandang yang berbeda, yang pertama berupa survei komprehensif dan yang kedua berupa rancangan sistem implementatif.

I. “Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges”

Artikel survei ini membahas tentang perkembangan e-voting berbasis blockchain secara global dan juga mengkaji bagaimana blockchain digunakan untuk menjaga keamanan, transparansi, auditabilitas, dan integritas suara. Blockchain dipandang mampu menjadi log transaksi yang tidak bisa diubah (immutable ledger). Jadi setiap suara tersimpan sebagai entri yang dapat diverifikasi dan dilacak perubahannya, sehingga manipulasi

pasca-pemungutan lebih mudah terdeteksi. Tetapi, solusi blockchain tidak otomatis siap dipakai untuk pemilu. Karena throughput transaction (berapa banyak suara per detik), latensi konfirmasi, dan juga biaya komputasi pada jaringan publik. Tidak hanya itu implementasi e-voting berbasis blockchain memerlukan infrastruktur digital yang matang dan juga prosedur operasional yang jelas. Dengan ledger semi-terbuka, pemantau independen bisa memverifikasi bahwa jumlah suara yang dihitung sesuai dengan suara yang direkam. Survei menegaskan bahwa transparansi seperti ini diproyeksikan dapat meningkatkan kepercayaan publik, karena warga tidak harus percaya ke satu instansi saja. Survei juga membahas tentang penggunaan teknik enkripsi homomorfik dan zero-knowledge proofs agar memastikan suara yang dihitung benar dan tidak membocorkan siapa memilih siapa. Intinya, artikel survei ini memposisikan blockchain sebagai solusi arsitektural untuk keamanan dan integritas e-voting, tapi juga menegaskan bahwa implementasi dunia nyata masih memiliki beberapa tantangan seperti skalabilitas, efisiensi, infrastruktur, dan regulasi.

II. "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization"

Artikel ini akan lebih membahas rancangan sistem konkret dengan blockchain public (Ethereum) dan smart contract. Tujuan utamanya adalah membuat suatu sistem voting online yang aman, transparan, dan meminimalkan ketergantungan pada pihak perantara. Dengan memanfaatkan blockchain Ethereum, setiap suara direkam melalui smart contract. Smart contract disini berfungsi sebagai aturan otomatis yang tidak bisa diubah secara sepihak setelah diterbitkan, sehingga mengurangi peluang manipulasi suara oleh pihak internal. Karena transaksi suara tersimpan di ledger blockchain, proses penghitungan dapat diaudit oleh publik. Transparansi ini bisa meningkatkan kepercayaan publik, karena hasil tidak hanya berasal dari klaim suatu instansi, tetapi dapat diverifikasi sendiri. Penulis artikel juga melakukan simulasi dengan dataset suara buatan untuk mengevaluasi tiga aspek, yaitu keamanan, skalabilitas, dan usability. Berdasarkan simulasi yang penulis artikel lakukan ditemukan bahwa masih ada tantangan signifikan untuk membawa sistem ke pemilu asli. Masalah terbesar dari sistem ini bukan hanya "apakah sistem yang digunakan aman?", tetapi juga kemauan masyarakat yang mau dan berani menggunakannya. Dari artikel ini juga menegaskan perlunya integrasi autentikasi pemilih berbasis data pemerintah dan juga biometrik. Hal ini memunculkan beberapa tantangan etis seperti siapa yang berhak mengakses data identitas pemilih.

III. "Online Voting in Ontario Municipalities: A Standards-Based Review"

Melalui Systematic Literature Review (SLR) dan survei terhadap 500 responden, penulis mengidentifikasi 5 dimensi transparansi, antara lain:

- Information Availability: Ketersediaan informasi publik seperti dokumentasi sistem, kode sumber, dan laporan audit.

- Understandability: Sejauh mana pemilih awam bisa memahami mekanisme sistem.
- Monitoring & Verifiability: Kemampuan publik atau auditor independen untuk memverifikasi integritas suara.
- Remedial Measures: Kesiapan sistem dalam menangani insiden keamanan.
- Testing: Pengujian publik. sebelum dilaksanakan pemilu

Temuan ini memperkuat bahwa transparansi merupakan faktor sosial yang dapat meningkatkan legitimasi demokrasi digital.

IV. **"A Symmetric, Probabilistic, Non-Circuit Based Fully Homomorphic Encryption Scheme"**

Artikel ini mengusulkan suatu sistem e-voting berbasis blockchain dengan kombinasi Elliptic Curve Cryptography dan SHA-256 hashing. Rancangan ini menekankan keamanan data dan privasi suara melalui tahap yaitu, autentikasi dan registrasi pemilih menggunakan enkripsi ECC, pencatatan suara di blockchain dengan hash SHA-256 untuk mencegah perubahan hasil, dan audit trail publik di blockchain yang nantinya dapat diverifikasi oleh pihak ketiga.

Penulis menekankan kalau sistem ini mampu mengurangi sentralisasi dan risiko manipulasi, serta menyediakan transparansi audit tanpa mengorbankan anonimitas pemilih. Namun ada juga beberapa tantangan utamanya seperti, skalabilitas blockchain publik, beban komputasi tinggi, dan kebutuhan infrastruktur server terdistribusi.

V. **"Development Of Audit and Data Protection Principles in Electronic Voting Systems"**

Artikel ini merancang suatu sistem e-voting menggunakan kombinasi RSA dan AES untuk melindungi proses pengiriman dan penyimpanan suara. Pada artikel ini penulis menerapkan hybrid cryptography dengan mekanisme RSA untuk kunci sesi, AES untuk enkripsi data suara, dan database terenkripsi untuk penyimpanan hasil pemungutan. Fokus dari artikel ini adalah integritas dan keaslian suara, tidak hanya transparansi. Penulis juga menyimpulkan bahwa sistem e-voting yang aman tidak selalu memerlukan blockchain, selama kombinasi algoritma dan protokol autentikasi mampu menjaga integritas, kerahasiaan, dan validitas suara.

3. Sintesis dan Kesenjangan Penelitian

Dari dua studi tersebut kita bisa tarik sebuah kesimpulan, blockchain diposisikan sebagai mekanisme teknis untuk menjaga integritas data suara karena bersifat immutable (tidak dapat diubah) jadi dapat mencegah manipulasi hasil setelah pemungutan suara. Tidak hanya itu smart contract juga dapat mengurangi intervensi manusia. Transparansi teknis dapat meningkatkan kepercayaan publik, dari dua artikel ini sama-sama mengklaim bahwa publik bisa memverifikasi suara secara terbuka, sehingga kepercayaan publik terhadap hasil pemilu akan naik. Kedua artikel juga sepakat bahwa jika tidak ada tata kelola, kebijakan, dan regulasi pemilu yang jelas,

solusi teknis masih belum cukup. Artinya kontribusi yang masih diperlukan yaitu, menganalisis bukan hanya arsitektur teknis saja, tetapi juga bagaimana kebijakan nasional, kesiapan infrastruktur, dan persepsi publik ikut menentukan apakah mekanisme keamanan benar-benar menjaga integritas pemilu.

4. Kerangka Konseptual Penelitian

Berdasarkan kajian literatur di atas, riset ini menggunakan kerangka berpikir bahwa keberhasilan pemilu digital yang aman dan dipercaya publik ditentukan oleh interaksi empat komponen:

1. **Teknologi Pengamanan Pemilu Digital**
2. **Keamanan Siber dan Integritas Data**
3. **Regulasi dan Tata Kelola**
4. **Kepercayaan Publik**

BAB III

METODOLOGI PENELITIAN

1. Desain Penelitian

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk menganalisis bagaimana mekanisme cyber security diterapkan dalam menjaga integritas data pada sistem pemilu digital. Pendekatan ini dipilih karena memungkinkan peneliti untuk mengidentifikasi, menilai, dan mensintesis hasil penelitian terdahulu secara sistematis guna memperoleh pemahaman yang komprehensif terkait tantangan, implementasi teknis, dan kebijakan yang berhubungan dengan keamanan siber dalam pemilu digital. Tujuan dari SLR ini adalah:

1. Mengidentifikasi tantangan utama dalam penerapan keamanan siber pada sistem pemilu digital.
2. Menilai pendekatan teknis dan strategi keamanan untuk menjaga integritas data dan mencegah manipulasi hasil pemilu digital.
3. Menganalisis hubungan antara regulasi, auditabilitas, dan tingkat kepercayaan publik terhadap sistem pemilu digital.

2. Strategi Pencarian dan Kriteria Penyaringan

Proses identifikasi literatur dilakukan melalui basis data **Scopus** dengan menggunakan string pencarian **“TITLE-ABS-KEY (("electronic voting" OR "e-voting" OR "online voting" OR "digital election system" OR "internet voting" OR "blockchain voting") AND ("cybersecurity" OR "data integrity" OR "information security" OR "data protection") AND ("implementation" OR "policy" OR "regulation" OR "trust" OR "public confidence" OR "governance")).** Pencarian dilakukan dengan mempertimbangkan relevansi terhadap topik penelitian, yaitu implementasi cyber security dalam menjaga integritas data pemilu digital. Proses penyaringan hasil pencarian dirangkum dalam Tabel 1 berikut.

Kriteria Penyaringan	Deskripsi	Jumlah Dokumen
String Pencarian	(("electronic voting" OR "e-voting" OR "online voting" OR "digital election system" OR "internet voting" OR "blockchain voting") AND ("cybersecurity" OR "data	118

	integrity" OR "information security" OR "data protection") AND ("implementation" OR "policy" OR "regulation" OR "trust" OR "public confidence" OR "governance"))	
Rentang Tahun	2018 hingga 2025	86
Area Subjek	Computer Science	71
Tipe Dokumen	Article, Conference Paper	59
Tahap Publikasi	Final	59
Bahasa	English	59
Open Access	All Open Access	14
TOTAL AWAL	**14 artikel dan prosiding**	
Sumber: diolah peneliti, Tahun		

Tabel 1. Pemilihan Sumber Data Berdasarkan Kriteria Penyaringan

3. Proses Screening dan Seleksi

Tahap screening dilakukan untuk memastikan kesesuaian setiap literatur dengan fokus penelitian, yaitu implementasi keamanan siber untuk menjaga integritas data pada pemilu digital. Proses ini dilakukan melalui dua tahapan utama:

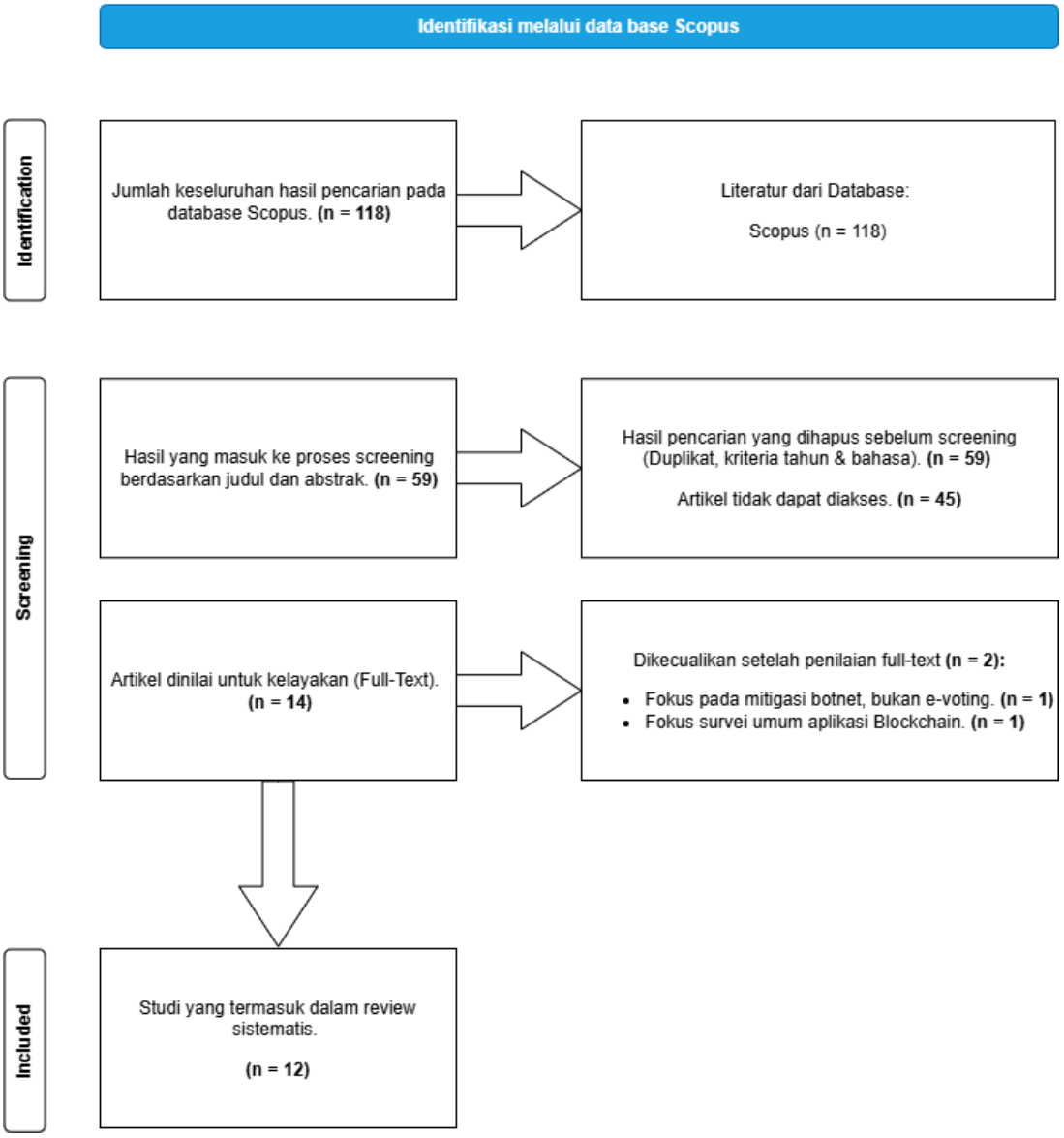
a. **Pemeriksaan Judul dan Abstrak:** Tahap ini menilai relevansi artikel terhadap topik penelitian. Artikel yang membahas keamanan data, kepercayaan publik, atau penerapan teknologi keamanan (seperti blockchain, enkripsi, atau autentikasi) dalam konteks e-voting akan dipertahankan.
b. **Analisis Full-Text:** Artikel yang lolos seleksi awal dianalisis secara menyeluruh untuk memastikan kesesuaian dengan kriteria inklusi. Analisis ini berfokus pada aspek implementasi teknis, kebijakan regulasi, dan mekanisme penguatan integritas data.

Berdasarkan proses tersebut, sebanyak 12 artikel dinyatakan memenuhi kriteria dan dilanjutkan ke tahap ekstraksi serta sintesis data. Jumlah ini sedikit

berbeda dari total awal karena adanya tahapan screening tambahan setelah penilaian full-text untuk memastikan kesesuaian fokus penelitian.

4. Diagram Alur Prisma

Tahapan seleksi artikel divisualisasikan melalui diagram alur PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses).



Gambar 1. Diagram Alur Seleksi Studi Berdasarkan Standar PRISMA

Perbedaan jumlah antara tabel penyaringan dan diagram PRISMA disebabkan oleh adanya tahap verifikasi tambahan pasca analisis full-text untuk memastikan literatur benar-benar relevan terhadap topik integritas data dalam sistem pemilu digital. Dengan demikian, hanya 12 artikel yang digunakan pada tahap ekstraksi dan sintesis.

5. Kriteria Inklusi dan Eksklusi

a. Kriteria Inklusi:

- Membahas sistem pemilu digital, electronic voting, atau e-voting.
- Menyoroti aspek keamanan siber, integritas data, auditabilitas, regulasi, atau kepercayaan publik.
- Menyertakan elemen implementasi teknis, studi kasus kebijakan, atau evaluasi sistem keamanan.

b. Kriteria Eksklusi:

- **R1.** Studi yang berfokus pada topik lain di luar e-voting, seperti e-government atau e-participation secara umum.
- **R2.** Artikel yang bersifat konseptual atau opini tanpa data implementatif.
- **R3.** Artikel yang tidak membahas aspek cyber security, data integrity, atau trust secara memadai.
- **R4.** Artikel yang tidak menyediakan informasi teknis yang cukup untuk mendukung analisis metodologi dan hasil.

6. Ekstraksi dan Sintesis Data

Data dari 12 artikel yang terpilih kemudian diekstraksi ke dalam template yang distandarisasi. Data yang diekstraksi meliputi:

1. Penulis dan Tahun Publikasi
2. Tujuan Penelitian
3. Metode atau Pendekatan Keamanan Siber
4. Aspek Keamanan yang Diterapkan (enkripsi, autentikasi, blockchain, audit, dsb.)
5. Fokus pada Integritas Data dan Kepercayaan Publik
6. Hasil dan Rekomendasi

Sintesis data dilakukan secara naratif dan tematik, dengan mengelompokkan temuan berdasarkan jenis teknologi keamanan, strategi penerapan, tantangan utama, serta kaitannya dengan regulasi dan kepercayaan publik terhadap sistem pemilu digital.

7. Title Literature Review

Title	Relevance	Key Point	Dipilih
Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals	Tinggi (Relevan dengan Rumusan Masalah 1, 2, 3)	Mengembangkan kerangka kerja keamanan siber holistik untuk e-Government. Memberikan dasar untuk struktur	YA
Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and	Sangat Tinggi (Relevan dengan Rumusan Masalah 1, 2)	Survei komprehensif mengenai arsitektur, solusi, dan tantangan penggunaan Blockchain untuk mengamankan sistem	YA
Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine	Sangat Tinggi (Relevan dengan Rumusan Masalah 2)	Fokus pada desain sistem e-voting yang aman, transparan, dan terdesentralisasi menggunakan Blockchain untuk mencegah manipulasi dan menjamin integritas data.	YA
An electoral exception? Quantum computing readiness and internet voting	Tinggi (Relevan dengan Rumusan Masalah 1)	Membahas kesiapan internet voting menghadapi ancaman keamanan di masa depan seperti Quantum Computing. Menyoroti tantangan keamanan yang	YA
Enhancing Security and Transparency in Online Voting through Blockchain Decentralization	Sangat Tinggi (Relevan dengan Rumusan Masalah 2)	Menjelaskan bagaimana Blockchain dapat meningkatkan keamanan dan transparansi (integritas data) dalam proses pemilu digital	YA
Blockchain-based e-voting system in a university	Tinggi (Relevan dengan Rumusan Masalah 2)	Menyajikan studi kasus dan implementasi praktis sistem e-voting berbasis Blockchain dalam skala kecil. Memberi contoh	YA
A Novel Electronic Voting Mechanism Based on Blockchain Technology	Tinggi (Relevan dengan Rumusan Masalah 2)	Mengusulkan mekanisme e-voting baru yang dirancang di atas teknologi Blockchain, berfokus pada fitur keamanan dan	YA
Evaluating the Public Perception of a Blockchain-Based Election	Rendah	Evaluasi terhadap persepsi dan kepercayaan publik terhadap pemilu berbasis Blockchain (aspek non-teknis).	TIDAK
Online Voting in Ontario Municipalities: A Standards-Based Review	Tinggi (Relevan dengan Rumusan Masalah 3)	(Relevan dengan RM 3)Meninjau online voting berdasarkan standar dan praktik terbaik. Relevan untuk membahas kerangka	YA
A Symmetric, Probabilistic, Non-Circuit Based Fully Homomorphic Encryption Scheme	Tinggi (Relevan dengan Rumusan Masalah 2)	Mengusulkan skema Enkripsi Homomorfik Penuh (FHE), teknik kriptografi canggih yang memungkinkan pemrosesan data terenkripsi untuk menjaga integritas dan	YA
DEVELOPMENT OF AUDIT AND DATA PROTECTION PRINCIPLES IN ELECTRONIC VOTING SYSTEMS	Sangat Tinggi (Relevan dengan Rumusan Masalah 2, 3)	Mengembangkan prinsip audit dan proteksi data yang spesifik untuk sistem pemilu digital. Kunci untuk pencegahan manipulasi	YA
Proactive Provenance Policies for Automatic Cryptographic Data Centric Security	Sedang	Fokus pada kebijakan proaktif untuk menjamin provena data (asal-usul data) dan keamanan data terpusat menggunakan kriptografi, namun tidak spesifik pada e-	TIDAK

Pada tahap akhir pemilihan kajian, tersisa 10 artikel inti yang dipilih dari total 12 artikel yang relevan, karena artikel-artikel ini menawarkan fokus pembahasan yang paling kuat dan langsung pada tiga pilar utama penelitian ini: Solusi Implementasi Teknis, Kerangka Kebijakan/Regulasi, dan Tantangan Keamanan dalam konteks Sistem Pemilu Digital.

BAB IV

HASIL ANALISA

1. **Tantangan utama dalam implementasi cyber security dalam sistem pemilu digital**

   Terdapat beberapa tantangan utama dalam implementasi cyber security dalam sistem pemilu digital, baik dari sisi teknis, operasional, maupun kepercayaan publik. Yang pertama ancaman keamanan teknis, sistem pemilu digital rentan terhadap berbagai ancaman, seperti kegagalan fungsi teknologi, rentan serangan, dan risiko diretas. Yang kedua masalah kepercayaan dan auditabilitas, munculnya kekhawatiran di kalangan warga bahwa mereka dapat kehilangan demokrasi jika menggunakan sistem pemungutan suara baru, hal ini karena mereka khawatir jika pemilu digital diperkenalkan audit yang luas dan tersedia bagi semua pemilih tidak mungkin ada. Yang ketiga skalabilitas dan kinerja, meningkatnya jumlah pemilih dapat memperlambat proses pemungutan suara serta dapat meningkatkan biaya.

2. **Implementasi keamanan data yang efektif untuk mencegah manipulasi**

   Implementasi keamanan data yang efektif pada sistem pemilu digital dilakukan melalui kombinasi teknologi enkripsi, autentikasi, dan audit. Enkripsi berlapis seperti AES dan RSA digunakan untuk melindungi data suara agar tidak mudah dimanipulasi, sementara autentikasi ganda memastikan hanya pemilih sah yang dapat mengakses sistem. Selain itu, penggunaan teknologi blockchain dapat menjaga integritas hasil dengan mencatat setiap suara secara transparan dan tidak dapat diubah. Audit berkala dan pemantauan sistem secara real-time juga diperlukan agar setiap aktivitas dapat dilacak sehingga potensi manipulasi dapat segera dideteksi dan dicegah.

3. **Peran regulasi pemerintah untuk memperkuat integritas data dan kepercayaan publik**

   Regulasi pemerintah berperan penting dalam memastikan keamanan dan keandalan pemilu digital. Pemerintah perlu menetapkan standar keamanan siber, kebijakan perlindungan data, serta mekanisme audit independen untuk menjamin transparansi proses pemilu. Selain itu, regulasi harus mengatur sanksi terhadap pelanggaran dan memastikan keterlibatan lembaga pengawas eksternal agar hasil pemilu dapat dipercaya. Dengan adanya kerangka hukum yang kuat dan pengawasan yang transparan, kepercayaan publik terhadap sistem pemilu digital dapat meningkat dan integritas data tetap terjaga.

BAB V

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa penerapan cyber security dalam sistem pemilu digital memiliki peran penting dalam menjaga integritas data serta kepercayaan publik terhadap hasil pemilu. Tantangan utama yang dihadapi meliputi ancaman teknis seperti peretasan dan kegagalan sistem, isu kepercayaan publik terhadap transparansi dan auditabilitas, serta kendala skalabilitas ketika jumlah pemilih meningkat.

Implementasi keamanan data yang efektif perlu memadukan teknologi enkripsi, autentikasi ganda, dan blockchain untuk memastikan setiap suara tersimpan aman dan tidak dapat dimanipulasi. Audit berkala serta pemantauan sistem secara real-time menjadi langkah penting untuk menjaga keaslian data suara.

Selain aspek teknis, regulasi pemerintah memiliki peran strategis dalam memperkuat keamanan dan integritas pemilu digital. Standar keamanan siber nasional, kebijakan perlindungan data, serta audit independen diperlukan untuk menciptakan sistem yang transparan dan akuntabel. Dengan sinergi antara teknologi yang kuat dan kebijakan yang jelas, pemilu digital dapat dilaksanakan secara aman, transparan, serta dipercaya oleh seluruh lapisan masyarakat.

DAFTAR PUSTAKA

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). *Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals*. International Journal of Information Security, 24(3), Article 121. https://doi.org/10.1007/s10207-025-01024-0

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., … Ibrahim, M. M. (2025). *Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges*. Cluster Computing, 28(2), Article 132. https://doi.org/10.1007/s10586-024-04709-8

Daraghmi, E., Hamoudi, A., & Abu Helou, M. (2024). *Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology in the context of Palestine*. Future Internet, 16(11), Article 388. https://doi.org/10.3390/fi16110388

Rodríguez-Pérez, A., Costa, N., & Finogina, T. (2024). *An electoral exception? Quantum computing readiness and internet voting*. eJournal of eDemocracy and Open Government, 16(3), 50–79. https://doi.org/10.29379/jedem.v16i3.928

Singh, I., Kaur, A., Agarwal, P., & Idrees, S. M. (2024). *Enhancing security and transparency in online voting through blockchain decentralization*. SN Computer Science, 5(7), Article 921. https://doi.org/10.1007/s42979-024-03286-2

Marouan, A., Badrani, M., Kannouf, N., Zannou, A., & Chetouani, A. (2024). *Blockchain-based e-voting system in a university*. Indonesian Journal of Electrical Engineering and Computer Science, 34(3), 1915–1923. https://doi.org/10.11591/ijeecs.v34.i3.pp1915-1923

Yang, C.-H., Su, P.-C., & Su, T.-C. (2023). *A novel electronic voting mechanism based on blockchain technology*. KSII Transactions on Internet and Information Systems, 17(10), 2862–2882. https://doi.org/10.3837/tiis.2023.10.015

Schiarelli, V., & Dupuis, M. (2023). *Evaluating the public perception of a blockchain-based election*. 157–163. https://doi.org/10.1145/3585059.3611439

Brunet, J., & Essex, A. (2023). *Online voting in Ontario municipalities: A standards-based review*. Lecture Notes in Computer Science, 14230 LNCS, 52–68. https://doi.org/10.1007/978-3-031-43756-4_4

Asante, G., Hayfron-Acquah, J. B., Asante, M., & Dagadu, J. C. (2022). *A symmetric, probabilistic, non-circuit based fully homomorphic encryption scheme*. International Journal of Computer Networks and Applications, 9(2), 160–168. https://doi.org/10.22247/ijcna/2022/212332

Khlaponin, Y., Vyshniakov, V., Ternavska, V., Sieliukov, O., & Komarnytskyi, O. (2021). *Development of audit and data protection principles in electronic voting systems*. Eastern-European Journal of Enterprise Technologies, 4(2-112), 47–57. https://doi.org/10.15587/1729-4061.2021.238259

Engram, S., Kaczmarek, T., Lee, A., & Bigelow, D. (2021). *Proactive provenance policies for automatic cryptographic data centric security*. Lecture Notes in Computer Science, 12839 LNCS, 71–87. https://doi.org/10.1007/978-3-030-80960-7_5