TESIS

SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN

(Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Kabupaten Madiun Jawa Timur)

Disusun oleh:

SYAIFUL HUDA

21.55.2179

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

TESIS

SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN

(Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

EMPLOYEE STATISTICAL DATA STORAGE SECURITY SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

(Case Study: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

Diajukan untuk memenuhi salah satu syarat mencapai derajat Pascasarjana
Program Studi PJJ Informatika

disusun oleh:

SYAIFUL HUDA
21.55.2179
Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN (Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

EMPLOYEE STATISTICAL DATA STORAGE SECURITY SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY (Case Study: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

yang disusun dan diajukan oleh

Syaiful Huda

21.55.2179

telah disetujui oleh Dosen Pembimbing Tesis
pada tanggal 3 November 2025

Dosen Pembimbing,

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PENGESAHAN

SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN

(Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

EMPLOYEE STATISTICAL DATA STORAGE SECURITY SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY (Case Study: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

yang disusun dan diajukan oleh

Syaiful Huda

21.55.2179

Telah dipertahankan di depan Dewan Penguji
pada tanggal 3 November 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Alva Hendi Muhammad, S.T., M.Eng., Ph.D. **NIK. 190302493**	
Robert Marco, S.T., M.T., Ph.D. **NIK. 190302228**	
Prof. Dr. Kusrini, M.Kom. **NIK. 190302106**	

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer
Tanggal 20 November 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Syaiful Huda
NIM : 21.55.2179
Konsentrasi : Digital Transformation Intelligence

Menyatakan bahwa Tesis dengan judul berikut:
SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN (Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)

Dosen Pembimbing Utama : Prof. Dr. Kusrini, M.Kom.
Dosen Pembimbing Pendamping : Kusnawi, S.Kom., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 3 November 2025
Yang Menyatakan,

Syaiful Huda

HALAMAN PERSEMBAHAN

Segala puji dan syukur saya panjatkan ke hadirat Allah SWT atas limpahan rahmat, taufik, dan hidayah-Nya.

Tesis ini saya persembahkan kepada:

1. **Bapak dan Ibu tercinta**,
   yang tak pernah lelah mendoakan, mendampingi, dan menyayangi saya dengan tulus dalam setiap proses kehidupan ini.
2. **Keluarga besar saya**,
   yang selalu memberi semangat, kehangatan, dan keyakinan untuk terus berjuang.

Semoga karya ini membawa keberkahan dan manfaat bagi kita semua.

HALAMAN MOTTO

Jika kamu tidak bisa membantu banyak orang, setidaknya jangan menyakiti mereka."

— **Prabowo Subianto**

"Ilmu tanpa amal adalah ibarat pohon tanpa buah."

— **Ali bin Abi Thalib**

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT yang telah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul:

"Sistem Keamanan Penyimpanan Data Statistik Kepegawaian Berbasis Teknologi Blockchain (Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia Pemerintah Kabupaten Madiun Jawa Timur)"

Tesis ini disusun sebagai salah satu syarat untuk memperoleh gelar Magister pada Program Studi S2 Teknik Informatika, Universitas Amikom Yogyakarta.

Penyusunan tesis ini tentu tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta;
2. Prof. Dr. Kusrini, M.Kom selaku pembimbing utama yang telah memberikan arahan, masukan, dan motivasi dalam proses penyusunan tesis ini.
3. Kusnawi, S.Kom., M.Eng selaku pembimbing pendamping yang senantiasa memberikan bimbingan teknis dan semangat dalam setiap tahapan penelitian.
4. Alva Hendi Muhammad, S.T., M.Eng., Ph.D. selaku Penguji 1;
5. Robert Marco, S.T., M.T., Ph.D. selaku Penguji 2;
6. Prof. Dr. Kusrini, M.Kom Selaku Penguji 3;
7. Dosen dan staf Pascasarjana Universitas Amikom Yogykarta, atas ilmu, dukungan, dan fasilitas yang diberikan selama masa studi.

8. Pemerintah Kabupaten Madiun, khususnya Badan Kepegawain dan Pengembangan Sumber Daya Manusia, yang telah memberikan data, informasi, dan dukungan dalam pelaksanaan penelitian.
9. Kepada keluarga tercinta, terutama bapak dan ibunda penulis, serta istri dan anak tercinta, atas doa, kasih sayang, dan dukungan moral yang tiada henti, yang menjadi sumber kekuatan dan semangat dalam menyelesaikan penelitian ini.
10. Seluruh pihak yang tidak dapat disebutkan satu per satu yang telah membantu secara langsung maupun tidak langsung dalam proses penyelesaian tesis ini.

Penulis menyadari bahwa tesis ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang.

Akhir kata, semoga tesis ini dapat memberikan manfaat dan kontribusi positif, baik bagi pengembangan ilmu pengetahuan maupun bagi penerapan teknologi di lingkungan pemerintahan daerah.

Yogyakarta, 3 November 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

Blockchain: Rangkaian blok data yang saling terhubung menggunakan teknologi kriptografi dan disimpan secara terdistribusi pada banyak node sehingga menjamin keamanan, transparansi, dan integritas data.

Ethereum Private: Versi privat dari jaringan Ethereum yang digunakan dalam lingkup organisasi atau instansi tertentu untuk membangun aplikasi berbasis blockchain dengan tingkat kontrol akses yang terbatas.

Smart Contract: Program atau protokol digital yang dijalankan di atas blockchain untuk mengatur, memverifikasi, dan mengeksekusi perjanjian atau transaksi secara otomatis sesuai aturan yang telah ditentukan.

Hashing (SHA-256): Proses transformasi data menjadi string unik dengan panjang tetap menggunakan algoritma SHA-256, yang digunakan untuk menjaga integritas dan keaslian data.

Middleware: Lapisan perangkat lunak perantara yang menghubungkan basis data relasional dengan blockchain, termasuk fungsi perhitungan hash, pengiriman data ke smart contract, serta verifikasi data.

Relational Database: Basis data yang menggunakan model relasional dengan tabel-tabel saling terhubung melalui kunci (primary key dan foreign key) untuk menyimpan dan mengelola data secara terstruktur.

Data Pegawai: Informasi terkait Aparatur Sipil Negara (ASN), yang meliputi Nomor Induk Pegawai (NIP), nama, unit kerja, jabatan, golongan, serta riwayat pendidikan.

Data Visualization (Visualisasi Data): Penyajian data dalam bentuk grafis, tabel, atau diagram interaktif yang memudahkan pengguna untuk memahami, menganalisis, dan mengambil keputusan berdasarkan data.

Good Governance: Prinsip tata kelola pemerintahan yang menekankan transparansi, akuntabilitas, partisipasi, efektivitas, serta supremasi hukum dalam penyelenggaraan administrasi publik.

Digital Audit Trail: Jejak digital yang merekam setiap aktivitas atau transaksi data dalam sistem, yang berguna sebagai bukti akuntabilitas dan kontrol untuk mencegah kecurangan atau manipulasi data.

INTISARI

Perkembangan sistem informasi kepegawaian di era digital menuntut adanya jaminan keamanan dan integritas data, khususnya pada data statistik kepegawaian yang menjadi dasar perencanaan, promosi, dan evaluasi sumber daya aparatur negara. Sistem konvensional berbasis basis data terpusat masih memiliki kelemahan berupa kerentanan terhadap manipulasi, risiko kehilangan data, dan keterbatasan kemampuan audit. Penelitian ini mengusulkan penerapan teknologi blockchain sebagai solusi untuk meningkatkan keamanan, transparansi, dan akuntabilitas pengelolaan data kepegawaian pada BKPSDM Kabupaten Madiun.

Model sistem yang dikembangkan mengimplementasikan blockchain permissioned (privat) berbasis Ethereum, di mana hanya node terotorisasi yang dapat memvalidasi transaksi dan menyimpan komitmen integritas data. Mekanisme keamanan dibangun melalui hashing kriptografis ganda menggunakan algoritma SHA-256 dan Keccak-256 (SHA-3), serta penyimpanan data terenkripsi pada basis data relasional off-chain, sedangkan nilai hash dicatat di blockchain (on-chain) sebagai bukti integritas digital.

Pengujian dilakukan dengan mengukur validasi hash, deteksi perubahan data (tamper detection), dan efisiensi sistem berdasarkan waktu eksekusi serta konsumsi sumber daya. Hasil penelitian menunjukkan bahwa sistem keamanan berbasis blockchain permissioned mampu menjaga integritas data dan mendeteksi perubahan secara otomatis. Algoritma Keccak-256 (SHA-3) menunjukkan efisiensi dan ketahanan yang lebih tinggi dibandingkan SHA-256, khususnya pada konteks blockchain privat di lingkungan pemerintahan. Penelitian ini menghasilkan prototipe sistem keamanan data terdistribusi yang transparan, auditabel, dan tahan manipulasi, serta berpotensi diterapkan untuk mendukung transformasi digital sistem kepegawaian pemerintah daerah.

Kata kunci: blockchain, keamanan data, kepegawaian, SHA-256, Keccak-256, Ethereum, integritas data.

ABSTRACT

The development of personnel information systems in the digital era requires guarantees of data security and integrity, particularly for civil service statistical data that serve as the foundation for planning, promotion, and evaluation of human resource policies. Conventional centralized database systems still have fundamental weaknesses, including susceptibility to manipulation, data loss, and limited auditability. This study proposes the implementation of blockchain technology as a solution to enhance the security, transparency, and accountability of personnel data management at the BKPSDM (Personnel and Human Resources Agency) of Madiun Regency.

The proposed system adopts a permissioned (private) blockchain architecture based on Ethereum, where only authorized nodes are allowed to validate transactions and record data integrity commitments. The security model employs dual cryptographic hashing mechanisms using SHA-256 and Keccak-256 (SHA-3), with encrypted personnel data stored in a relational off-chain database, while the hash values are recorded on-chain as digital integrity proofs.

Testing and evaluation were conducted through hash validation, tamper detection, and system efficiency measurement based on execution time and resource consumption. The results show that the proposed permissioned blockchain system effectively maintains data integrity and automatically detects data modifications. The Keccak-256 (SHA-3) algorithm demonstrated higher efficiency and resilience compared to SHA-256, particularly in the context of private blockchain environments within government institutions. This research produces a distributed data security prototype that is transparent, auditable, and tamper-resistant, contributing to the digital transformation and secure management of civil service information systems in local government agencies.

Keyword: *blockchain, data security, personnel system, SHA-256, Keccak-256, Ethereum, data integrity.*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi di era digital membawa dampak signifikan terhadap sistem pengelolaan data pemerintahan, termasuk dalam bidang manajemen kepegawaian. Data statistik kepegawaian menjadi salah satu komponen penting dalam proses perencanaan, promosi, dan penilaian kinerja Aparatur Sipil Negara (ASN), sehingga memerlukan sistem penyimpanan data yang aman, konsisten, dan dapat diverifikasi.

Namun, sistem informasi kepegawaian yang digunakan saat ini seringkali masih bergantung pada arsitektur basis data terpusat (centralized database) yang menyimpan seluruh data dalam satu server utama. Model ini memiliki kelemahan utama, antara lain rentan terhadap manipulasi data, kehilangan data akibat kegagalan sistem, serta sulitnya proses audit integritas secara menyeluruh (Sari et al., 2021). Kondisi tersebut dapat menimbulkan risiko serius terhadap validitas data kepegawaian yang menjadi dasar kebijakan strategis dalam pengelolaan sumber daya manusia di pemerintahan.

Untuk mengatasi permasalahan tersebut, berbagai pendekatan keamanan data telah dikembangkan, termasuk kriptografi, hashing, dan mekanisme audit digital. Salah satu teknologi yang efektif dalam menjamin integritas dan transparansi data adalah blockchain. Teknologi ini menyimpan data dalam bentuk blok-blok yang saling terhubung (linked blocks) melalui fungsi hash kriptografis

sehingga setiap perubahan data dapat terdeteksi secara otomatis (Xingjie & Huaqun, 2022). Selain itu, blockchain bersifat terdistribusi dan immutable, sehingga data yang telah tercatat tidak dapat dimodifikasi tanpa persetujuan node yang berwenang (Han et al., 2022).

Studi terkini menunjukkan bahwa blockchain berpotensi besar di sektor publik untuk meningkatkan keamanan, transparansi, dan akuntabilitas pengelolaan data. Laporan Komisi Eropa (Tangi et al., 2022) menegaskan bahwa penerapan blockchain dalam administrasi publik memberikan efisiensi tinggi dalam verifikasi data, mengurangi duplikasi, serta mempermudah audit digital. Dalam konteks kepegawaian, blockchain permissioned (privat) menjadi solusi ideal karena memungkinkan pembatasan akses hanya bagi pihak berwenang serta mendukung proses validasi data yang aman dan dapat dilacak (Judijanto, 2023).

Lebih lanjut, kemajuan algoritma kriptografi modern membuka peluang penerapan fungsi hash ganda untuk memperkuat mekanisme keamanan. SHA-256 telah lama menjadi standar pada sistem kripto seperti Bitcoin, sementara Keccak-256 (SHA-3)—dengan struktur sponge function—dirancang lebih tahan terhadap serangan tertentu, termasuk kolisi dan diferensial (Al-Azzam et al., 2023). Kombinasi dan perbandingan kedua algoritma ini penting untuk mengukur efektivitasnya dalam konteks pemerintahan, di mana kecepatan dan keandalan verifikasi data menjadi faktor krusial.

Selain aspek keamanan, penerapan blockchain juga membangun transparansi dan kepercayaan publik. Rahman et al. (2023) menunjukkan bahwa sistem blockchain privat meningkatkan akuntabilitas administrasi publik karena

setiap transaksi atau perubahan data tercatat secara permanen dan tidak dapat dihapus. Hal ini relevan bagi pemerintah daerah untuk menjamin bahwa perubahan data pegawai—misalnya mutasi, kenaikan pangkat, atau pembaruan status—dapat ditelusuri dan diverifikasi cepat tanpa celah manipulasi.

Berdasarkan kondisi tersebut, penelitian ini berfokus pada pengembangan model sistem keamanan penyimpanan data statistik kepegawaian berbasis blockchain privat Ethereum pada studi kasus BKPSDM Kabupaten Madiun (Jawa Timur). Model dirancang untuk menjamin keaslian, integritas, dan keamanan data melalui pencatatan terdistribusi yang sulit dimanipulasi. Penelitian ini menerapkan dan membandingkan SHA-256 dan Keccak-256 (SHA-3) dalam proses verifikasi untuk menilai efisiensi, performa, dan ketahanan terhadap manipulasi data, sehingga dapat diidentifikasi algoritma paling optimal untuk menjaga integritas informasi. Lebih jauh, penelitian ini menyajikan bukti empiris efektivitas blockchain dalam memperkuat keamanan data sektor publik melalui sistem yang terdistribusi, transparan, dan auditabel. Kontribusi utama penelitian meliputi prototipe sistem berbasis Ethereum permissioned dengan verifikasi ganda berbasis hash, analisis komparatif, serta hasil uji empiris yang dapat menjadi rujukan ilmiah maupun pedoman praktis bagi instansi pemerintah daerah.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan menerapkan model sistem keamanan penyimpanan data statistik kepegawaian berbasis teknologi blockchain

permissioned (privat) yang mampu menjamin keaslian, integritas, dan auditabilitas data melalui mekanisme hashing kriptografis dan penyimpanan terdistribusi?

2. Bagaimana perbandingan tingkat efisiensi, performa, dan ketahanan keamanan antara algoritma hash SHA-256 dan Keccak-256 (SHA-3) dalam menjaga integritas serta mendeteksi perubahan (tampering) data pada sistem blockchain permissioned berbasis Ethereum?

1.3 Batasan Masalah

Untuk menjaga fokus dan kedalaman analisis dalam penelitian ini, maka ruang lingkup penelitian dibatasi pada hal-hal berikut:

1. Penelitian ini hanya difokuskan pada perancangan dan implementasi sistem keamanan penyimpanan data statistik kepegawaian berbasis teknologi blockchain permissioned (privat) menggunakan platform Ethereum.
2. Aspek keamanan yang dikaji dibatasi pada penerapan dan perbandingan dua algoritma hash kriptografis, yaitu SHA-256 dan Keccak-256 (SHA-3), yang digunakan untuk menjamin integritas dan keaslian data antara penyimpanan off-chain (basis data MariaDB terenkripsi) dan on-chain (ledger blockchain).
3. Penelitian ini tidak membahas aspek antarmuka pengguna, integrasi sistem kepegawaian nasional, maupun kebijakan implementasi dan biaya infrastruktur. Fokus penelitian terbatas pada model arsitektur keamanan, mekanisme enkripsi dan hashing, serta pembuktian integritas data melalui

smart contract dalam konteks sistem kepegawaian pemerintah daerah (BKPSDM Kabupaten Madiun).

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan model sistem keamanan penyimpanan data statistik kepegawaian berbasis teknologi blockchain permissioned (privat) menggunakan platform Ethereum, yang mampu menjamin keaslian, integritas, dan auditabilitas data melalui penerapan mekanisme hashing kriptografis serta penyimpanan data terenkripsi secara off-chain.
2. Menganalisis dan membandingkan tingkat efisiensi, performa, serta ketahanan keamanan antara algoritma hash SHA-256 dan Keccak-256 (SHA-3) dalam menjaga integritas dan keaslian data pada sistem blockchain permissioned berbasis Ethereum, khususnya dalam konteks pengelolaan data statistik kepegawaian di lingkungan instansi pemerintah.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan sistem informasi dan teknologi blockchain, khususnya dalam konteks penerapan mekanisme hashing kriptografis (SHA-256 dan Keccak-256/SHA-3) untuk menjamin integritas dan keaslian data.

2. Memberikan solusi teknis bagi instansi pemerintah, khususnya BKPSDM Kabupaten Madiun, dalam meningkatkan keamanan, transparansi, dan auditabilitas data kepegawaian melalui penerapan teknologi blockchain.
3. Menyediakan prototipe sistem keamanan penyimpanan data terdistribusi yang dapat diadaptasi untuk mendukung transformasi digital dan tata kelola data aparatur yang lebih aman dan efisien.
4. Menunjukkan efektivitas algoritma Keccak-256 (SHA-3) dibandingkan SHA-256 dalam menjaga integritas data pada lingkungan blockchain permissioned, sehingga dapat menjadi acuan pemilihan algoritma kriptografis yang tepat untuk sistem pemerintahan.

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian mengenai penerapan sistem informasi dalam pengelolaan data kepegawaian telah banyak dilakukan, terutama dalam konteks digitalisasi dan keamanan data. Namun, penerapan teknologi blockchain dalam bidang ini masih terbilang baru, khususnya dalam lingkup pemerintahan daerah. Tinjauan terhadap beberapa studi sebelumnya menjadi penting untuk melihat posisi serta kontribusi dari penelitian ini.

Penelitian yang dilakukan oleh Al-Azzam et al. (2023) dalam *MDPI Electronics* berfokus pada analisis komparatif implementasi algoritma Keccak (SHA-3) dalam berbagai lingkungan sistem, baik berbasis perangkat lunak maupun perangkat keras. Studi ini menyoroti aspek efisiensi dan keamanan hash function Keccak terhadap serangan kolisi dan manipulasi data. Hasil pengujian menunjukkan bahwa Keccak-256 memiliki performa hashing yang tinggi dan konsumsi sumber daya yang relatif rendah, menjadikannya sangat cocok untuk penerapan pada sistem blockchain permissioned. Meskipun begitu, penelitian ini belum menyentuh konteks penggunaan Keccak-256 dalam penyimpanan data pemerintahan. Relevansi penelitian ini terhadap tesis adalah pada penerapan Keccak-256 sebagai mekanisme integritas data dalam sistem penyimpanan data kepegawaian berbasis blockchain privat.

Sementara itu, studi oleh Choudhary et al. (2023) dalam *SPIE Conference Proceedings* mengulas penggunaan algoritma hash dan tanda tangan digital pada dua ekosistem blockchain besar: Bitcoin dan Ethereum. SHA-256 digunakan dalam Bitcoin, sedangkan Keccak-256 digunakan dalam Ethereum. Studi ini menjelaskan bagaimana kedua algoritma tersebut bekerja dalam menjaga integritas transaksi dan otentikasi digital. SHA-256 terbukti efisien dalam sistem proof-of-work, sementara Keccak-256 lebih fleksibel dan cocok untuk penerapan smart contract. Penelitian ini bersifat analisis teoretis dan belum diuji pada domain data pemerintahan. Keterkaitannya dengan tesis ini adalah bahwa mekanisme hash dan tanda tangan digital yang dibahas menjadi pondasi penting dalam merancang sistem blockchain untuk keamanan data pegawai.

Penelitian oleh Majeed et al. (2023) yang diterbitkan di *MDPI Applied Sciences* mengusulkan kerangka kerja verifikasi dokumen digital berbasis integrasi IPFS dan blockchain Ethereum. Penelitian ini mengimplementasikan konsep *hash-on-chain* (hash disimpan di blockchain) dan *data-off-chain* (dokumen disimpan di IPFS) untuk menjaga integritas sekaligus efisiensi penyimpanan. Hasilnya menunjukkan bahwa sistem ini dapat memverifikasi keaslian dokumen tanpa perlu membuka isi data, sehingga menjaga kerahasiaan dan transparansi. Walaupun belum diterapkan di instansi pemerintahan, model ini sangat relevan untuk penerapan sistem penyimpanan data statistik kepegawaian, di mana data pegawai yang sensitif harus diamankan namun tetap dapat diaudit.

Sharma et al. (2023) melalui publikasi *arXiv preprint* memperkenalkan sistem bernama Verifi-Chain, yang berfungsi sebagai platform verifikasi kredensial

menggunakan teknologi blockchain dan IPFS. Penelitian ini memanfaatkan hash function untuk menghasilkan sidik jari digital yang unik bagi setiap dokumen yang diverifikasi. Prototipe yang dikembangkan menunjukkan bahwa sistem mampu mencegah pemalsuan dan perubahan data dengan memastikan bahwa setiap hash dokumen sesuai dengan data aslinya. Walaupun studi ini masih terbatas dalam skala pengujian, konsep hash-based verification yang diterapkan memberikan landasan yang kuat untuk verifikasi data pegawai secara otomatis dalam sistem kepegawaian berbasis blockchain. Penelitian oleh Wardhana (2024) berfokus pada analisis potensi blockchain dalam meningkatkan keamanan database kependudukan di Kementerian Dalam Negeri. Hasil penelitian menunjukkan bahwa blockchain mampu mencegah manipulasi data dan memastikan keandalan informasi melalui mekanisme verifikasi terdistribusi. Namun, penelitian ini terbatas pada tinjauan konseptual dan belum melakukan pengujian empiris terhadap performa sistem blockchain yang diusulkan. Penelitian ini relevan karena memperlihatkan potensi penerapan blockchain pada data publik berskala besar, yang kemudian diadaptasi dalam penelitian ini untuk konteks data kepegawaian di pemerintahan daerah.

Dalam penelitian Dewi et al. (2025) yang dipublikasikan pada *AIP Conference Proceedings*, dikembangkan sistem verifikasi dokumen aman menggunakan blockchain Ethereum privat, IPFS, dan enkripsi Threefish. Penelitian ini berfokus pada keamanan ganda antara integritas data (melalui hash) dan kerahasiaan (melalui enkripsi). Hasil pengujian menunjukkan bahwa integritas dokumen tetap terjaga meskipun dilakukan proses enkripsi dan penyimpanan terdistribusi. Namun, penelitian ini tidak membandingkan efektivitas algoritma

hash lain seperti SHA-256 atau Keccak-256. Dalam tesis ini, pendekatan tersebut diperluas dengan analisis komparatif dua algoritma hash untuk menentukan mana yang paling efektif menjaga keamanan data kepegawaian dalam blockchain privat.

Penelitian oleh Rachman et al. (2025) dari *Universitas Pendidikan Indonesia* meneliti penerapan Keccak-256 dan tanda tangan digital ECDSA untuk validasi e-sertifikat berbasis blockchain. Tujuan utama penelitian ini adalah memastikan keaslian dan integritas dokumen elektronik dengan menggunakan hash function dan digital signature. Hasil implementasi menunjukkan bahwa Keccak-256 mampu mendeteksi perubahan data dengan sangat akurat, sementara ECDSA menjamin keaslian penerbit dokumen. Meski pengujian efisiensi pada data skala besar belum dilakukan, pendekatan ini dapat diadaptasi pada sistem kepegawaian untuk validasi data ASN dan dokumen pegawai digital yang tersimpan dalam blockchain.

Terakhir, Raharjo et al. (2025) melalui publikasi di *J-PTIIK Universitas Brawijaya* meneliti implementasi blockchain permissioned untuk sistem e-voting. Penelitian ini menekankan pentingnya mekanisme konsensus dan hashing dalam menjaga integritas suara pemilih agar tidak dapat dimanipulasi. Sistem diuji melalui berbagai skenario, termasuk duplikasi dan perubahan data, dan hasilnya menunjukkan bahwa blockchain permissioned mampu mencegah manipulasi dan menjaga transparansi data. Walaupun fokus penelitian ini adalah e-voting, prinsip keamanan data terdistribusi dan mekanisme hash verification yang digunakan memiliki kemiripan langsung dengan kebutuhan keamanan data statistik kepegawaian dalam sistem pemerintahan.

Berdasarkan hasil telaah terhadap Dari delapan penelitian di atas, dapat disimpulkan bahwa penerapan blockchain untuk menjamin integritas dan keamanan data digital telah banyak diuji di berbagai domain seperti sertifikat, dokumen, dan e-voting. Namun, penerapan khusus pada sistem data kepegawaian terutama yang berbasis blockchain privat dan menggunakan perbandingan algoritma hash (SHA-256 dan Keccak-256) belum banyak dilakukan. Oleh karena itu, penelitian ini menempati posisi penting dalam mengisi celah tersebut dengan pendekatan teknis komparatif dan implementatif yang berorientasi pada kebutuhan keamanan data aparatur sipil negara di pemerintahan daerah.

Selain itu, sebagian besar penelitian sebelumnya tidak membahas penerapan blockchain di lingkungan pemerintahan daerah, padahal instansi seperti Badan Kepegawaian dan Pengembangan Sumber Daya Manusia (BKPSDM) sangat bergantung pada validitas data kepegawaian untuk pengambilan keputusan strategis, promosi jabatan, dan pelayanan publik. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan mengembangkan prototipe sistem keamanan penyimpanan data statistik kepegawaian berbasis blockchain privat Ethereum, yang memanfaatkan dua algoritma hash (SHA-256 dan Keccak-256) untuk memverifikasi integritas data secara berlapis.

2.2 Keaslian Penelitian

Tabel 2.1. Matriks literatur review dan posisi penelitian
SISTEM KEAMANAN PENYIMPANAN DATA STATISTIK KEPEGAWAIAN BERBASIS TEKNOLOGI BLOCKCHAIN
(Studi Kasus: Badan Kepegawaian Dan Pengembangan Sumber Daya Manusia
Pemerintah Kabupaten Madiun Provinsi Jawa Timur)

No	Judul Penelitian	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Comparative Study of Keccak (SHA-3) Implementations	Al-Azzam et al., *MDPI Electronics*, 2023	Menganalisis efisiensi dan keamanan algoritma Keccak pada sistem blockchain.	Keccak-256 efisien, fleksibel, dan tahan kolisi, cocok untuk sistem blockchain privat.	Tidak diuji dalam konteks data pemerintahan.	Penelitian ini menerapkan Keccak-256 untuk menjaga integritas data kepegawaian dalam blockchain privat.
2	Comparative Analysis of Cryptographic Hash Functions in Blockchain Systems	Singh & Patel, *CEUR Workshop Proceedings*, 2023	Membandingkan performa hash (SHA-2, SHA-3, BLAKE2) untuk sistem blockchain.	Keccak-256 unggul dari sisi keamanan, SHA-256 unggul dalam kestabilan.	Tidak diuji secara praktis pada sistem penyimpanan data.	Penelitian ini menguji langsung kedua algoritma hash pada data kepegawaian.
3	Digital Signature and Hash Algorithms Used in Bitcoin and Ethereum	Choudhary et al., *SPIE Conf. Proc.*, 2023	Mengkaji implementasi SHA-256 (Bitcoin) dan Keccak-256 (Ethereum) dalam	Kedua algoritma memiliki kekuatan tinggi dalam menjamin integritas data.	Analisis teoretis tanpa simulasi sistem data.	Penelitian ini mengadaptasi pendekatan tersebut ke sistem data pegawai untuk validasi integritas.

No	Judul Penelitian	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			keamanan transaksi blockchain.			
4	IPFS-Blockchain Smart Contracts Framework for Certificate Verification	Majeed et al., *MDPI Applied Sciences*, 2023	Merancang sistem verifikasi sertifikat berbasis blockchain dan IPFS.	Model hash-on-chain dan data-off-chain menjamin integritas dokumen.	Pengujian terbatas, belum diterapkan di sektor publik.	Penelitian ini menerapkan konsep serupa pada penyimpanan data statistik ASN secara aman dan efisien.
5	Verifi-Chain: A Credentials Verifier using Blockchain and IPFS	Sharma et al., *arXiv Preprint*, 2023	Membangun sistem verifikasi dokumen menggunakan hash dan penyimpanan terdistribusi IPFS.	Hash terbukti efektif mendeteksi manipulasi data.	Belum diuji pada data skala besar.	Pendekatan verifikasi hash ini diadaptasi untuk sistem keamanan data kepegawaian.
6	Secure Document Verification using Blockchain and IPFS with Threefish Encryption	Dewi et al., *AIP Conf. Proc.*, 2025	Mendesain sistem verifikasi dokumen terenkripsi menggunakan blockchain privat.	Hash dan enkripsi menjamin integritas & kerahasiaan data.	Tidak membandingkan algoritma hash yang berbeda.	Penelitian ini memperluas konsep dengan membandingkan SHA-256 dan Keccak-256 pada data pegawai.

No	Judul Penelitian	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
7	Validasi E-Certificate menggunakan Keccak-256 dan ECDSA di Blockchain	Rachman et al., *UPI Repository*, 2025	Menerapkan hash Keccak-256 dan ECDSA untuk autentikasi e-sertifikat.	Hash Keccak-256 efektif menjaga keaslian data digital.	Uji efisiensi sistem belum dilakukan pada data kompleks.	Penelitian ini menerapkan Keccak-256 untuk validasi hash data statistik kepegawaian.
8	Implementasi Permissioned Blockchain untuk E-Voting	Raharjo et al., *J-PTIIK UB*, 2025	Menjamin integritas data suara dengan blockchain permissioned.	Hash dan konsensus berhasil mencegah manipulasi data.	Domain terbatas pada e-voting.	Prinsip integritas yang sama diterapkan pada penyimpanan data ASN untuk memastikan keamanan.

2.3 Landasan Teori

2.3.1 Sistem Informasi Kepegawaian

Sistem informasi kepegawaian merupakan salah satu bentuk penerapan teknologi informasi di sektor publik yang bertujuan untuk meningkatkan efisiensi dan efektivitas pengelolaan sumber daya manusia aparatur sipil negara (ASN). Menurut Yulianto, Kartika, & Rahmawati (2020), sistem informasi kepegawaian terintegrasi dapat membantu pemerintah daerah dalam mengelola data pegawai secara lebih sistematis, mulai dari rekrutmen, penempatan, mutasi, promosi, hingga pensiun. Sistem ini tidak hanya berfungsi sebagai penyimpanan data administratif, tetapi juga sebagai basis pengetahuan untuk mendukung pengambilan keputusan strategis.

Namun, dalam praktiknya masih banyak tantangan yang dihadapi, seperti keterpencaran data antar instansi, inkonsistensi format, keterlambatan pembaruan, hingga keterbatasan dalam keamanan data (BPS, 2023). Hal ini dapat mengurangi keakuratan analisis kebutuhan pegawai, menimbulkan risiko duplikasi atau manipulasi data, serta memperlambat proses pengambilan kebijakan berbasis bukti (evidence-based policy making).

Oleh karena itu, dibutuhkan sistem informasi kepegawaian yang tidak hanya terintegrasi secara fungsional antarlembaga, tetapi juga dilengkapi dengan mekanisme keamanan yang kuat untuk menjamin keaslian dan integritas data. Pada titik inilah pemanfaatan teknologi blockchain menjadi relevan, karena mampu menghadirkan sistem yang lebih transparan, aman, dan akuntabel.

2.3.2 Keamanan Data (Data Security)

Keamanan data (data security) merupakan aspek fundamental dalam pengelolaan sistem informasi yang bertujuan untuk melindungi data dari ancaman yang dapat mengakibatkan kerusakan, kehilangan, kebocoran, atau penyalahgunaan informasi. Prinsip dasar keamanan data mencakup tiga komponen utama yang dikenal dengan istilah CIA Triad, yaitu Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) (Whitman & Mattord, 2022). Confidentiality menjamin bahwa data hanya dapat diakses oleh pihak yang memiliki otorisasi; Integrity memastikan data tidak diubah tanpa izin atau manipulasi; sedangkan Availability menjamin bahwa data selalu tersedia dan dapat digunakan oleh pengguna yang berhak kapan pun dibutuhkan. Dalam konteks sistem kepegawaian, penerapan prinsip CIA ini menjadi sangat penting karena data pegawai mengandung informasi sensitif seperti identitas pribadi, riwayat jabatan, hingga data remunerasi, yang jika bocor dapat menimbulkan risiko hukum, reputasi, dan kepercayaan publik terhadap lembaga pemerintah.

Selain CIA Triad, konsep keamanan data modern juga mencakup aspek Authentication (autentikasi), Authorization (otorisasi), dan Non-repudiation (tidak dapat disangkal) (Stallings, 2021). Autentikasi berfungsi memastikan bahwa pengguna yang mengakses sistem benar-benar teridentifikasi, sedangkan otorisasi membatasi hak akses berdasarkan peran atau jabatan. Non-repudiation menjamin bahwa setiap tindakan atau transaksi digital dapat ditelusuri kembali ke pelakunya, sehingga tidak dapat disangkal oleh pihak mana pun. Dalam sistem kepegawaian pemerintahan, ketiga aspek tambahan ini mendukung audit trail yang transparan

dan akuntabel, terutama dalam proses administrasi kepegawaian seperti mutasi, promosi, atau penilaian kinerja.

Dalam era digital saat ini, ancaman terhadap keamanan data pemerintahan semakin kompleks. Menurut laporan Badan Siber dan Sandi Negara (BSSN, 2023), terdapat lebih dari 400 juta serangan siber yang menargetkan sistem digital pemerintah di Indonesia, termasuk serangan ransomware, SQL injection, dan data breach terhadap server kepegawaian daerah. Hal ini menunjukkan bahwa model penyimpanan data yang masih bersifat terpusat (centralized system) memiliki risiko tinggi terhadap kebocoran dan manipulasi data, terutama bila tidak didukung oleh enkripsi dan manajemen akses yang kuat.

Untuk mengatasi permasalahan tersebut, teknologi blockchain menawarkan pendekatan baru dalam menjaga keamanan data melalui arsitektur terdistribusi dan mekanisme kriptografi yang kuat. Setiap data yang disimpan dalam blockchain dilindungi dengan hash function dan disebarkan ke seluruh node jaringan, sehingga sangat sulit dimanipulasi tanpa terdeteksi. Selain itu, sistem consensus mechanism memastikan bahwa setiap perubahan data hanya dapat dilakukan jika disetujui oleh seluruh node yang berwenang. Dengan karakteristik ini, blockchain mampu memperkuat aspek integrity dan non-repudiation, yang menjadi kelemahan utama dalam sistem kepegawaian konvensional berbasis server pusat (Crosby et al., 2016).

Oleh karena itu, dalam konteks penelitian ini, keamanan data dipandang tidak hanya sebagai perlindungan terhadap akses tidak sah, tetapi juga sebagai kemampuan sistem untuk menjamin keaslian, keterlacakan, dan keandalan data pegawai secara menyeluruh. Pendekatan ini menjadi dasar bagi penerapan

teknologi blockchain permissioned berbasis Ethereum privat dalam sistem keamanan penyimpanan data statistik kepegawaian terintegrasi, guna meningkatkan perlindungan dan integritas data di lingkungan BKPSDM Kabupaten Madiun.

2.3.3 Teknologi Blockchain

Blockchain merupakan teknologi penyimpanan data terdistribusi yang berfungsi sebagai buku besar digital (distributed ledger) yang mencatat transaksi atau informasi secara permanen dalam bentuk blok-blok yang saling terhubung dan diamankan melalui algoritma kriptografi (Nakamoto, 2008). Setiap blok dalam jaringan blockchain berisi hash kriptografi dari blok sebelumnya, timestamp, dan data transaksi. Keterhubungan ini membentuk rantai (chain) data yang tidak dapat diubah tanpa mengubah seluruh blok berikutnya, menjadikannya immutable (tidak dapat dimodifikasi) dan transparent (dapat diverifikasi oleh seluruh node jaringan) (Crosby et al., 2016).

Prinsip kerja blockchain didasarkan pada tiga komponen utama, yaitu desentralisasi, transparansi, dan keamanan kriptografi.

1. Desentralisasi berarti tidak ada otoritas tunggal yang mengendalikan seluruh sistem; setiap node dalam jaringan memiliki salinan data yang sama.
2. Transparansi memungkinkan setiap perubahan data dapat dilacak dan diverifikasi oleh semua pihak yang berwenang.
3. Keamanan kriptografi menjamin bahwa setiap transaksi atau perubahan data divalidasi melalui mekanisme konsensus seperti Proof of Work (PoW),

Proof of Stake (PoS), atau Practical Byzantine Fault Tolerance (PBFT) (Zheng et al., 2017).

Berdasarkan hak akses dan mekanisme kontrolnya, blockchain diklasifikasikan menjadi tiga jenis utama (Yli-Huumo et al., 2016):

1. Public Blockchain – jaringan terbuka yang dapat diakses oleh siapa pun tanpa batasan, contohnya Bitcoin dan Ethereum publik.
2. Private Blockchain – jaringan tertutup yang dikelola oleh satu entitas, di mana kontrol akses bersifat sentral, biasanya digunakan oleh perusahaan atau organisasi internal.
3. Permissioned Blockchain – jaringan semi-tertutup yang hanya memperbolehkan entitas tertentu untuk bergabung dan berpartisipasi dalam proses validasi transaksi, dengan sistem otorisasi yang jelas.

Dalam konteks pemerintahan dan sistem kepegawaian, permissioned blockchain menjadi pilihan paling tepat karena memiliki keseimbangan antara keamanan, privasi, dan efisiensi. Hanya pihak-pihak yang berwenang seperti BKPSDM, Badan Kepegawaian Negara (BKN), dan Inspektorat Daerah yang diberikan izin untuk mengakses, memvalidasi, atau memperbarui data pegawai. Model ini memastikan bahwa data tetap terdistribusi antar instansi, tetapi tidak dapat diakses publik tanpa izin, sehingga mendukung prinsip confidentiality dan integrity dari keamanan data.

Selain itu, blockchain mendukung penggunaan smart contract, yaitu potongan kode logika bisnis yang berjalan otomatis ketika kondisi tertentu terpenuhi. Dalam sistem kepegawaian, smart contract dapat digunakan untuk

mengotomatiskan validasi data pegawai, pencatatan kenaikan pangkat, atau pengesahan dokumen digital secara aman tanpa intervensi manual (Zhu & Zhou, 2021). Dengan demikian, blockchain tidak hanya berfungsi sebagai penyimpanan data yang aman, tetapi juga sebagai mekanisme otomatisasi proses administrasi yang transparan dan terpercaya.

Teknologi blockchain juga mendukung prinsip traceability (ketertelusuran) dan auditability (kemampuan diaudit). Setiap transaksi yang terjadi akan tercatat secara permanen di seluruh node jaringan dan dapat ditelusuri kapan pun tanpa risiko penghapusan data. Hal ini sangat relevan bagi sistem kepegawaian pemerintah, di mana audit data pegawai sering diperlukan dalam pengawasan dan evaluasi.

Dalam penelitian ini digunakan blockchain permissioned berbasis Ethereum privat, di mana jaringan blockchain dibangun dalam lingkungan tertutup yang hanya dapat diakses oleh pihak yang memiliki otorisasi. Model ini memungkinkan setiap transaksi data kepegawaian dicatat secara terenkripsi menggunakan cryptographic hashing dan divalidasi melalui mekanisme konsensus PBFT (Practical Byzantine Fault Tolerance). Dengan pendekatan ini, sistem diharapkan mampu menjamin keaslian (authenticity), integritas (integrity), dan ketahanan terhadap manipulasi (tamper-resistance) data kepegawaian secara terintegrasi lintas instansi.

2.3.4 Arsitektur Blockchain

Arsitektur blockchain merupakan kerangka teknis yang menjelaskan bagaimana suatu sistem blockchain dibangun, diorganisasikan, dan beroperasi

sebagai buku besar terdistribusi (distributed ledger). Melalui arsitektur ini, blockchain mampu menjamin keamanan, transparansi, efisiensi, dan keandalan data dalam suatu jaringan digital. Menurut Zheng et al. (2017), arsitektur blockchain secara umum terdiri atas empat lapisan utama, yaitu lapisan data (data layer), lapisan jaringan (network layer), lapisan konsensus (consensus layer), dan lapisan aplikasi (application layer). Keempat lapisan ini saling berinteraksi untuk memastikan integritas sistem secara menyeluruh.

1. Lapisan Data (Data Layer)

   Lapisan data berfungsi sebagai pondasi utama dalam sistem blockchain. Pada lapisan ini, data disimpan dalam bentuk blok-blok yang saling terhubung melalui hash kriptografi. Struktur blok terdiri dari dua bagian:

   a. Header, berisi hash dari blok sebelumnya, timestamp, dan nonce;
   b. Body, berisi data transaksi atau catatan aktivitas.

   Keterhubungan antarblok menjadikan blockchain bersifat immutable, artinya data yang telah dicatat tidak dapat diubah tanpa memengaruhi seluruh rantai blok (Nakamoto, 2008). Dalam konteks pemerintahan, lapisan data dapat digunakan untuk mencatat riwayat ASN (Aparatur Sipil Negara), seperti pangkat, jabatan, diklat, dan sertifikasi. Catatan digital tersebut menjadi jejak permanen (audit trail) yang menjamin keaslian data kepegawaian.

2. Lapisan Jaringan (Network Layer)

   Lapisan jaringan bertanggung jawab atas komunikasi antar node dalam sistem blockchain. Node-node ini berfungsi untuk menyiarkan, memverifikasi,

dan menyimpan transaksi menggunakan protokol peer-to-peer (P2P) (Crosby et al., 2016).

Dalam konteks pemerintahan, node dapat dikelola oleh berbagai instansi, misalnya:

a. Badan Kepegawaian Negara (BKN) sebagai node pusat,
b. BKPSDM provinsi dan kabupaten/kota sebagai node verifikator daerah,
c. Kementerian PANRB dan BPSDM sebagai node pengawas dan pengelola kebijakan.

Model komunikasi P2P ini memastikan sinkronisasi data kepegawaian secara otomatis di seluruh jaringan pemerintah, tanpa ketergantungan pada satu server pusat.

3. Lapisan Konsensus (Consensus Layer)

Lapisan konsensus merupakan mekanisme yang memastikan seluruh node memiliki kesepakatan terhadap validitas transaksi sebelum data dimasukkan ke blockchain. Beberapa mekanisme konsensus yang dikenal antara lain:

a. Proof of Work (PoW), yang berbasis komputasi;
b. Proof of Stake (PoS), berbasis kepemilikan;
c. Practical Byzantine Fault Tolerance (PBFT) dan Istanbul Byzantine Fault Tolerance (IBFT), yang berbasis kesepakatan antar node terpercaya (Xie et al., 2019).

Untuk kebutuhan sistem pemerintahan, algoritma PBFT atau IBFT lebih sesuai karena:

a. Efisien dalam waktu verifikasi,
b. Tidak memerlukan energi besar seperti PoW,
c. Hanya memperbolehkan node resmi yang memiliki otoritas validasi.

Dengan mekanisme ini, keabsahan setiap perubahan data kepegawaian dapat dipastikan melalui konsensus lintas instansi tanpa risiko manipulasi.

4. Lapisan Aplikasi (Application Layer)

Lapisan aplikasi merupakan antarmuka bagi pengguna untuk berinteraksi dengan sistem blockchain. Pada lapisan ini, berbagai aplikasi terdesentralisasi (Decentralized Applications/DApps) dapat dikembangkan sesuai kebutuhan birokrasi.

Komponen utama lapisan aplikasi mencakup:

a. Smart Contract, yaitu program otomatis yang mengeksekusi kebijakan atau aturan administrasi tanpa intervensi manual;
b. API (Application Programming Interface), yang menghubungkan blockchain dengan sistem eksternal seperti SIASN atau e-Kinerja;
c. Antarmuka pengguna (User Interface), yang menyediakan akses visual dan fungsional bagi ASN maupun publik.

Contohnya, proses usulan kenaikan pangkat ASN dapat dilakukan secara otomatis melalui smart contract, yang hanya mengeksekusi persetujuan bila semua syarat administratif telah terpenuhi dan diverifikasi oleh node-node terkait (BKPSDM dan BKN).

2.3.5 Arsitektur Sistem Informasi di Pemerintahan

Arsitektur sistem informasi pemerintahan, yang juga dikenal sebagai Government Enterprise Architecture atau arsitektur e-government, merupakan kerangka kerja terpadu yang dirancang untuk mendukung tata kelola pemerintahan berbasis teknologi informasi dan komunikasi (TIK). Tujuan utama dari arsitektur ini adalah memastikan interoperabilitas antar sistem, efisiensi pengelolaan sumber daya digital, serta konsistensi data dan layanan publik di seluruh instansi pemerintahan (Kominfo, 2022).

1. Lapisan Layanan (Service Layer)

   Lapisan ini berfokus pada penyediaan berbagai layanan digital kepada masyarakat, pegawai pemerintah, maupun entitas eksternal seperti pelaku usaha. Contohnya adalah layanan kepegawaian daring, perizinan terpadu, dan portal layanan publik. Lapisan ini berperan sebagai antarmuka antara sistem pemerintahan dan pengguna akhir, sehingga menuntut desain yang user-friendly, aman, dan responsif.

2. Lapisan Aplikasi (Application Layer)

   Lapisan ini menampung berbagai aplikasi pemerintahan yang menjalankan fungsi-fungsi operasional, seperti sistem kepegawaian (SIASN), keuangan (SAKTI), administrasi umum, hingga perencanaan daerah (SIPD). Integrasi antar aplikasi dilakukan melalui middleware atau application programming interface (API) agar pertukaran data antar instansi berjalan lancar. Dengan demikian, lapisan ini menjadi kunci dalam mewujudkan interoperabilitas antar sistem pemerintahan.

3. Lapisan Data (Data Layer)

Lapisan data bertugas mengelola seluruh informasi dan basis data pemerintahan, baik yang bersifat transaksional maupun strategis. Data dapat tersimpan secara terpusat di pusat data nasional (PDN) atau secara terdistribusi di masing-masing instansi, tergantung pada kebijakan tata kelola data. Prinsip utama dalam lapisan ini adalah data governance, yang menekankan aspek kualitas data, keamanan, dan aksesibilitas yang terkendali.

4. Lapisan Infrastruktur (Infrastructure Layer)

Lapisan ini mencakup seluruh komponen fisik dan jaringan yang mendukung operasional sistem pemerintahan, seperti server, perangkat penyimpanan, jaringan komunikasi, pusat data nasional, dan cloud computing. Pemerintah Indonesia melalui inisiatif PDN berupaya menyediakan infrastruktur yang andal, aman, dan efisien sebagai fondasi utama ekosistem digital nasional (Kominfo, 2022).

Meskipun arsitektur sistem informasi pemerintahan telah menunjukkan kemajuan signifikan, model yang masih bersifat terpusat (centralized) memiliki sejumlah kelemahan. Sistem terpusat berpotensi menimbulkan risiko single point of failure, yang berarti apabila terjadi gangguan pada pusat data utama, maka seluruh layanan dapat terhenti. Selain itu, struktur ini rentan terhadap serangan siber, kebocoran data, serta manipulasi administratif yang dapat menurunkan kepercayaan publik terhadap sistem digital pemerintah (Setiawan & Ramdhani, 2023).

Dalam konteks inilah, integrasi teknologi blockchain menjadi solusi inovatif untuk memperkuat arsitektur sistem informasi pemerintahan. Blockchain memungkinkan data disimpan secara terdistribusi di banyak node, dengan setiap transaksi tercatat secara transparan dan tidak dapat diubah (immutable). Dengan menerapkan pendekatan ini, sistem pemerintahan dapat memperoleh manfaat berupa:

a. Keamanan tinggi, karena setiap perubahan data harus diverifikasi oleh seluruh node jaringan.
b. Transparansi dan akuntabilitas, karena semua transaksi dapat dilacak secara publik maupun internal.
c. Desentralisasi pengendalian, yang mengurangi ketergantungan pada satu entitas pengelola.
d. Efisiensi audit dan pelacakan data, melalui mekanisme pencatatan berbasis ledger digital.

Oleh karena itu, penggabungan arsitektur e-government dengan teknologi blockchain melahirkan paradigma baru yang disebut Government Blockchain Architecture (GBA) — sebuah model yang mengintegrasikan prinsip keterbukaan data, keamanan digital, dan tata kelola terdistribusi dalam sistem informasi pemerintahan modern.

2.3.6 Fungsi Hash Kriptografis

Fungsi hash kriptografis adalah algoritma yang mengubah input data dengan panjang variabel menjadi output tetap (hash value) yang bersifat unik dan tidak dapat dikembalikan (one-way function). Hash digunakan untuk memastikan

integritas dan keaslian data, karena perubahan sekecil apa pun pada data asli akan menghasilkan nilai hash yang berbeda (Rahman et al., 2023).

Sifat penting fungsi hash kriptografis (NIST, 2021):

1. Deterministik: input yang sama selalu menghasilkan hash yang sama.
2. Avalanche Effect: perubahan kecil pada input menghasilkan perubahan besar pada hash.
3. Pre-image Resistance: sulit menemukan input yang menghasilkan hash tertentu.
4. Collision Resistance: sangat kecil kemungkinan dua input berbeda menghasilkan hash yang sama.

Dalam blockchain, setiap blok berisi hash blok sebelumnya; perubahan data pada satu blok otomatis merusak rantai berikutnya. Oleh karena itu, hash berperan penting dalam menjaga immutability data.

2.3.7 Algoritma SHA-256 dan Keccak-256 (SHA-3)

SHA-256 (Secure Hash Algorithm 256-bit) Dikembangkan oleh NIST tahun 2001, SHA-256 merupakan bagian dari keluarga SHA-2. Algoritma ini menghasilkan hash sepanjang 256 bit dan digunakan secara luas dalam sistem blockchain seperti Bitcoin. SHA-256 memiliki tingkat keamanan tinggi dan struktur internal berbasis Merkle–Damgård, namun relatif lebih lambat di perangkat lunak dibandingkan versi modern (NIST, 2021).

Keccak-256 (SHA-3) adalah versi standar SHA-3 yang disetujui oleh NIST pada 2015. Algoritma ini menggunakan sponge function, yang menjadikannya lebih fleksibel dan tahan terhadap serangan diferensial maupun kolisi (Al-Azzam et al.,

2023). Keccak-256 banyak digunakan dalam Ethereum blockchain, termasuk untuk pembuatan alamat wallet dan identifikasi smart contract.

2.3.8 Model Keamanan Sistem (STRIDE dan DREAD)

Dalam perancangan sistem keamanan berbasis blockchain, dibutuhkan pendekatan sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi potensi ancaman serta risiko keamanan. Salah satu metode yang banyak digunakan dalam pengembangan sistem modern adalah threat modeling, yaitu proses untuk memahami ancaman potensial dan merancang langkah mitigasinya sejak tahap desain sistem (Shostack, 2014).

Penelitian ini menggunakan dua pendekatan populer, yaitu STRIDE untuk identifikasi ancaman dan DREAD untuk analisis tingkat risiko. Kedua model ini digunakan secara komplementer agar sistem keamanan blockchain permissioned dapat dirancang dengan mempertimbangkan mitigasi ancaman secara menyeluruh (Howard & LeBlanc, 2002; Shostack, 2014).

a. Model STRIDE

Model STRIDE dikembangkan oleh Microsoft sebagai kerangka kerja untuk mengidentifikasi berbagai jenis ancaman terhadap sistem informasi. Akronim STRIDE mewakili enam kategori utama, yaitu Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, dan Elevation of Privilege (Microsoft, 2022; Shostack, 2014).

Kategori STRIDE	Jenis Ancaman	Penjelasan dan Relevansi

S – Spoofing Identity	Pemalsuan identitas pengguna atau node sistem.	Penyerang berpura-pura menjadi entitas sah untuk memperoleh akses ke jaringan blockchain permissioned.
T – Tampering with Data	Manipulasi atau perubahan data tanpa izin.	Terjadi ketika data diubah sebelum proses hashing atau selama transmisi antara off-chain dan on-chain.
R – Repudiation	Penolakan terhadap tindakan yang telah dilakukan.	Pengunggah data menyangkal pernah mengirim data tanpa bukti digital yang valid.
I – Information Disclosure	Pengungkapan data sensitif kepada pihak tidak berwenang.	Ancaman berupa kebocoran data kepegawaian akibat kelemahan enkripsi.
D – Denial of Service (DoS)	Gangguan sistem dengan membanjiri jaringan.	Serangan yang menghambat validasi blok atau akses smart contract.

E – Elevation of Privilege	Peningkatan hak akses tanpa otorisasi.	Pengguna biasa mengeksploitasi celah untuk menjadi admin atau validator.

Model STRIDE digunakan dalam fase identifikasi ancaman (threat identification). Pada penelitian ini, setiap komponen sistem — seperti smart contract, node validator, gateway, dan basis data off-chain — dievaluasi terhadap keenam kategori ancaman tersebut.

Implementasi mitigasi STRIDE dalam penelitian ini meliputi:

1. Spoofing → mitigasi dengan autentikasi digital dan smart contract berbasis peran (RBAC).
2. Tampering → mitigasi dengan penggunaan hash ganda (SHA-256 dan Keccak-256) dan ledger immutable.
3. Repudiation → mitigasi dengan pencatatan event transaksi otomatis pada blockchain.
4. Information Disclosure → mitigasi dengan enkripsi AES-256-GCM dan pengelolaan kunci melalui KMS.
5. Denial of Service → mitigasi melalui pembatasan node (Proof of Authority) dan firewall jaringan.
6. Elevation of Privilege → mitigasi dengan validasi hak akses dan batasan fungsi di smart contract.

Pendekatan STRIDE membantu mengidentifikasi ancaman sejak tahap desain arsitektur, yang sangat penting dalam sistem berbasis blockchain permissioned (Chakraborty & Chen, 2022).

b. Model DREAD

Model DREAD digunakan untuk mengukur tingkat risiko keamanan dengan memberikan penilaian kuantitatif terhadap ancaman yang telah diidentifikasi menggunakan STRIDE. DREAD adalah akronim dari Damage Potential, Reproducibility, Exploitability, Affected Users, dan Discoverability (Howard & LeBlanc, 2002).

Parameter DREAD	Deskripsi
D – Damage Potential	Seberapa besar kerusakan yang ditimbulkan jika ancaman berhasil dieksploitasi.
R – Reproducibility	Seberapa mudah serangan dapat diulang atau direplikasi.
E – Exploitability	Seberapa mudah celah keamanan dapat dimanfaatkan oleh penyerang.
A – Affected Users	Jumlah pengguna yang terdampak oleh serangan.
D – Discoverability	Seberapa mudah celah keamanan ditemukan oleh pihak luar.

Masing-masing parameter diberi nilai skala 1–10, dan nilai rata-rata digunakan untuk menentukan tingkat risiko:

1. 1–3 = Risiko rendah (Low Risk)
2. 4–6 = Risiko sedang (Medium Risk)

3. 7–10 = Risiko tinggi (High Risk)

Dalam konteks penelitian ini, model DREAD digunakan untuk menilai tingkat risiko dari ancaman STRIDE terhadap sistem blockchain permissioned.

Contohnya:

1. Ancaman Spoofing Identity bernilai tinggi (karena berdampak langsung pada keabsahan transaksi).
2. Tampering Data bernilai sedang karena termitigasi oleh hash ganda.
3. Repudiation bernilai rendah karena blockchain memiliki non-repudiation property (Zheng et al., 2018).

2.3.9 Sistem Keamanan Data Kepegawaian Berbasis Blockchain

Sistem keamanan data kepegawaian berbasis blockchain bertujuan untuk memastikan bahwa setiap data pegawai yang disimpan dan diproses bersifat otentik, terverifikasi, dan tidak dapat diubah. Model sistem ini terdiri dari dua lapisan:

1. Off-chain layer: basis data relasional tempat data utama pegawai disimpan.
2. On-chain layer: jaringan blockchain yang mencatat hash data dan metadata transaksi.

Setiap kali data pegawai diperbarui, sistem akan menghasilkan hash baru (misalnya SHA-256 dan Keccak-256) yang disimpan ke blockchain. Proses verifikasi dilakukan dengan membandingkan hash yang tersimpan di blockchain dengan hash baru hasil input data. Jika identik, data dianggap valid; jika berbeda, maka ada indikasi perubahan tidak sah.

Pendekatan ini sejalan dengan penelitian Sari et al. (2021) yang membuktikan bahwa integrasi blockchain dalam sistem administrasi pemerintahan

dapat meningkatkan akurasi dan keamanan penyimpanan data sensitif. Dalam penelitian ini, kombinasi dua algoritma hash digunakan untuk menilai efisiensi, performa, dan ketahanan sistem dalam mendeteksi manipulasi data kepegawaian secara real-time.

BAB III

METODE PENELITIAN

3.1 Jenis, Sifat, dan Pendekatan Penelitian

3.1.1 Jenis Penelitian

Jenis penelitian ini merupakan penelitian eksperimental rekayasa perangkat lunak (software engineering experimental research) yang berfokus pada pembangunan dan pengujian prototipe sistem keamanan data berbasis blockchain permissioned. Dalam penelitian ini, diterapkan dua algoritma hash kriptografis, yaitu SHA-256 dan Keccak-256 (SHA-3), untuk menilai efisiensi proses hashing, ketahanan sistem terhadap manipulasi data, serta kemampuan sistem dalam mendeteksi perubahan atau tamper detection. Melalui pendekatan eksperimental, penelitian ini memungkinkan dilakukan pengujian langsung terhadap performa dan efektivitas mekanisme keamanan yang diusulkan, sehingga hasilnya dapat memberikan bukti empiris mengenai kemampuan model dalam menjaga integritas dan keaslian data statistik kepegawaian.

3.1.2 Sifat Penelitian

Penelitian ini bersifat aplikatif dan komparatif. Sifat aplikatif terlihat dari hasil penelitian yang berupa model sistem keamanan terapan yang dapat diimplementasikan secara langsung pada sistem informasi kepegawaian BKPSDM Kabupaten Madiun. Sifat komparatif ditunjukkan melalui perbandingan kinerja dua algoritma hash kriptografis, yaitu SHA-256 dan Keccak-256 (SHA-3), dalam menjaga integritas dan efisiensi sistem. Perbandingan tersebut dilakukan

berdasarkan waktu proses hashing, konsumsi sumber daya sistem, serta akurasi sistem dalam mendeteksi manipulasi data, sehingga diperoleh algoritma yang paling optimal untuk diterapkan dalam konteks blockchain permissioned.

3.1.3 Pendekatan Penelitian

Pendekatan penelitian yang digunakan adalah eksperimental rekayasa sistem keamanan berbasis hashing ganda (Dual Cryptographic Hashing Security Engineering Approach). Pendekatan ini diawali dengan analisis kebutuhan dan risiko keamanan pada sistem konvensional yang masih terpusat, kemudian dilanjutkan dengan perancangan model keamanan menggunakan dua lapisan hashing, yaitu SHA-256 untuk verifikasi di sisi off-chain dan Keccak-256 (SHA-3) untuk validasi di sisi on-chain. Setelah itu dilakukan implementasi prototipe sistem pada jaringan Ethereum permissioned dengan mekanisme konsensus Proof of Authority (PoA). Prototipe yang dibangun kemudian diuji dan dievaluasi untuk menilai efisiensi, integritas, serta kemampuan sistem dalam mendeteksi perubahan data secara otomatis. Hasil pengujian dianalisis untuk menarik kesimpulan mengenai efektivitas mekanisme hashing ganda dalam menjaga keaslian dan integritas data statistik kepegawaian. Pendekatan ini memastikan sistem yang dikembangkan mampu memberikan lapisan keamanan berlapis melalui verifikasi hash ganda yang mendeteksi setiap perubahan data secara kriptografis.

3.2 Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini menggunakan beberapa pendekatan yang saling melengkapi untuk mendukung proses analisis kebutuhan, perancangan sistem, serta pengujian model keamanan berbasis blockchain. Teknik

pengumpulan data yang digunakan meliputi studi literasi dan dokumentasi, yang dijelaskan sebagai berikut:

3.2.1 Studi Literasi

Studi literasi dilakukan dengan cara mengumpulkan, menelaah, dan menganalisis berbagai sumber ilmiah yang relevan dengan topik penelitian, baik berupa buku, jurnal internasional, prosiding konferensi, laporan penelitian, maupun publikasi resmi dari instansi pemerintah dan lembaga akademik. Kegiatan ini bertujuan untuk memperoleh landasan teoritis dan konseptual yang kuat mengenai sistem informasi kepegawaian, termasuk struktur data dan alur manajemen Aparatur Sipil Negara (ASN), teknologi blockchain dan penerapannya pada sektor publik, smart contract sebagai mekanisme otomatisasi validasi data, serta algoritma hashing kriptografi khususnya SHA-256 dan Keccak-256 dalam konteks keamanan data. Selain itu, kajian juga mencakup integrasi blockchain dengan basis data relasional (hybrid architecture) untuk penyimpanan data kepegawaian, serta konsep good governance, transparansi, dan akuntabilitas publik dalam tata kelola data pemerintah daerah.

Melalui studi literasi ini, peneliti berupaya mengidentifikasi kesenjangan penelitian (research gap) dalam penerapan blockchain untuk keamanan data ASN, memperkuat kerangka teori, serta memastikan bahwa penelitian memiliki dasar ilmiah yang valid dan aplikatif. Hasil dari studi literasi ini selanjutnya menjadi pedoman dalam menentukan parameter pengujian performa algoritma hash, merancang arsitektur sistem blockchain privat, serta menyusun mekanisme validasi data hash antar-blok yang digunakan dalam penelitian ini.

3.2.2 Dokumentasi

Metode dokumentasi dilakukan dengan cara mengumpulkan data sekunder dari instansi terkait, yaitu Badan Kepegawaian dan Pengembangan Sumber Daya Manusia (BKPSDM) Kabupaten Madiun. Data yang dikumpulkan meliputi data statistik kepegawaian yang mencakup status kepegawaian (Pegawai Negeri Sipil/PNS, Pegawai Pemerintah dengan Perjanjian Kerja/PPPK, dan Calon Pegawai Negeri Sipil/CPNS), unit kerja atau Organisasi Perangkat Daerah (OPD) tempat pegawai bertugas, jabatan dan golongan ruang baik struktural maupun fungsional, serta tingkat pendidikan sebagai indikator kualifikasi dan kompetensi pegawai.

Data tersebut digunakan untuk memahami kondisi eksisting sistem informasi kepegawaian, mengidentifikasi permasalahan pada aspek keamanan dan integritas data, serta menjadi dasar dalam perancangan model sistem keamanan berbasis teknologi blockchain. Selain itu, data yang diperoleh juga dimanfaatkan sebagai dataset uji dalam proses implementasi sistem, khususnya untuk melakukan hashing data menggunakan algoritma SHA-256 dan Keccak-256, menyimpan hasil hash ke dalam jaringan blockchain privat, serta melakukan validasi dan visualisasi hasil pada dashboard sistem yang dikembangkan.

3.3 Metode Analisis Data

Metode analisis data dalam penelitian ini difokuskan untuk menilai efektivitas model keamanan berbasis blockchain permissioned dalam menjaga integritas dan keaslian data statistik kepegawaian. Pendekatan analisis dilakukan secara deskriptif kualitatif yang dikombinasikan dengan analisis teknis kuantitatif,

sehingga hasil penelitian mencerminkan baik aspek konseptual maupun performa aktual dari sistem keamanan yang diimplementasikan.

Pendekatan ini dipilih karena sistem yang dikembangkan bukan hanya berorientasi pada kinerja teknis, tetapi juga pada keandalan model keamanan dalam menjamin bahwa setiap data yang disimpan tidak dapat dimanipulasi, dihapus, atau diubah tanpa jejak digital yang terverifikasi.

3.3.1 Analisis Deskriptif Kualitatif

Analisis deskriptif kualitatif digunakan untuk memahami secara mendalam mekanisme pengelolaan data kepegawaian yang sedang berjalan serta menilai kontribusi model blockchain permissioned terhadap peningkatan keamanan data. Langkah-langkah analisis mencakup:

1. Analisis Proses Bisnis dan Alur Data Kepegawaian
   a. Mengidentifikasi alur penyimpanan dan distribusi data statistik pegawai (jumlah, jabatan, usia, pendidikan, golongan).
   b. Menggambarkan proses verifikasi dan pelaporan dalam sistem konvensional yang masih terpusat di server BKPSDM.
2. Identifikasi Kelemahan Sistem Eksisting Analisis dilakukan terhadap kelemahan-kelemahan sistem terpusat yang berpotensi menurunkan integritas dan keaslian data, seperti:
   a. Potensi manipulasi atau pengubahan data tanpa audit trail,
   b. Keterbatasan otorisasi dan autentikasi pengguna,
   c. Risiko kehilangan data akibat gangguan server atau akses tidak sah.

3. Evaluasi Konseptual Model Keamanan Blockchain. Berdasarkan hasil studi literasi dan observasi lapangan, analisis difokuskan pada bagaimana blockchain permissioned:
    a. Menciptakan ledger digital yang immutable (tidak dapat diubah),
    b. Menjamin integritas data melalui pencatatan hash kriptografis (SHA-256 dan Keccak-256),
    c. Memastikan keaslian data dengan validasi terdistribusi antar-node terotorisasi,
    d. Menyediakan jejak audit permanen (digital audit trail) melalui smart contract dan event log transaksi.

Analisis kualitatif ini menghasilkan pemetaan hubungan antara kelemahan sistem konvensional dan solusi keamanan yang diberikan oleh model blockchain permissioned, sehingga dapat dinilai relevansinya terhadap konteks pengelolaan data kepegawaian di BKPSDM.

3.3.2 Analisis Teknis Kuantitatif

Analisis teknis kuantitatif dilakukan untuk mengukur tingkat efektivitas dan efisiensi model keamanan yang dikembangkan, terutama dalam aspek integritas dan keaslian data. Pengujian difokuskan pada kinerja dua algoritma hash kriptografis, SHA-256 dan Keccak-256 (SHA-3), sebagai fondasi verifikasi integritas digital dalam blockchain.

Fokus analisis mencakup empat parameter utama:

1. Integritas Data (Data Integrity Validation)

2. Menguji konsistensi nilai hash antara data asli (off-chain) dengan hash yang tercatat di blockchain (on-chain).
3. Nilai hash yang identik menunjukkan data terjaga keasliannya, sedangkan perbedaan menandakan adanya perubahan atau manipulasi.
4. Proses ini membuktikan kemampuan sistem dalam menjaga integritas data statistik kepegawaian secara otomatis.
5. Keaslian Data (Data Authenticity)
    a. Diuji melalui fungsi smart contract yang mencatat identitas pengguna, waktu transaksi, dan hash data.
    b. Setiap perubahan hanya dapat dilakukan oleh entitas berotorisasi (node validator), sehingga seluruh transaksi bersifat non-repudiable (tidak dapat disangkal).
6. Waktu Proses Hashing dan Transaksi (Performance Efficiency)
    a. Mengukur waktu hashing untuk berbagai ukuran data, serta waktu pencatatan hash ke blockchain permissioned.
    b. Hasil pengujian dibandingkan antara SHA-256 dan Keccak-256 untuk menentukan algoritma paling efisien dan cocok digunakan dalam sistem pemerintahan.
7. Ketahanan terhadap Manipulasi (Tamper Detection)
    a. Data diubah sebagian secara sengaja di basis data relasional, kemudian sistem diuji apakah mampu mendeteksi perubahan tersebut.
    b. Indikator keberhasilan: sistem mengeluarkan status "data tidak valid" karena nilai hash berbeda dari yang tercatat di blockchain.

Hasil pengujian disajikan dalam tabel komparatif dan grafik untuk menampilkan performa algoritma hash, efisiensi sistem, serta tingkat keberhasilan deteksi manipulasi data.

3.4 Alur Penelitian

Alur penelitian ini menggambarkan langkah sistematis dari analisis kebutuhan hingga penarikan kesimpulan, dengan inti mekanisme hashing kriptografis ganda SHA-256 (off-chain) dan Keccak-256/SHA-3 (on-chain) untuk menjamin integritas dan keaslian data statistik kepegawaian pada lingkungan blockchain permissioned (Ethereum, PoA) digambarkan pada gambar 3.1.

1. Analisis Kebutuhan dan Risiko Sistem Konvensional

   Analisis ini bertujuan memetakan kelemahan sistem berbasis basis data terpusat, khususnya risiko manipulasi data, kehilangan data, dan keterbatasan jejak audit. Kegiatan dilakukan melalui studi literatur, telaah dokumen, serta observasi alur data di BKPSDM.

2. Perancangan Model Keamanan Hashing Ganda

   Perancangan ini bertujuan membangun arsitektur hibrida yang memadukan penyimpanan off-chain terenkripsi dengan pencatatan komitmen on-chain. Desain menyertakan enkripsi AES-256-GCM yang dikelola KMS melalui envelope encryption untuk data off-chain, penetapan SHA-256 sebagai local integrity hash atas ciphertext di sisi off-chain dan Keccak-256 sebagai on-chain commitment yang native di EVM, serta perancangan smart contract yang mencakup RBAC, fungsi storeDataHash, verifyHash, dan event log

3. Implementasi Prototipe pada Ethereum Permissioned (PoA)

Implementasi ini bertujuan mewujudkan rancangan dalam lingkungan uji yang terkontrol dan representatif. Kegiatan meliputi penyiapan jaringan private Ethereum (GoQuorum atau Besu) dengan konsensus Proof of Authority, pengembangan smart contract berbasis Solidity dan middleware untuk enkripsi, hashing, serta koneksi node, serta penyusunan basis data MariaDB terenkripsi untuk menyimpan ciphertext beserta authentication tag dan envelope key.

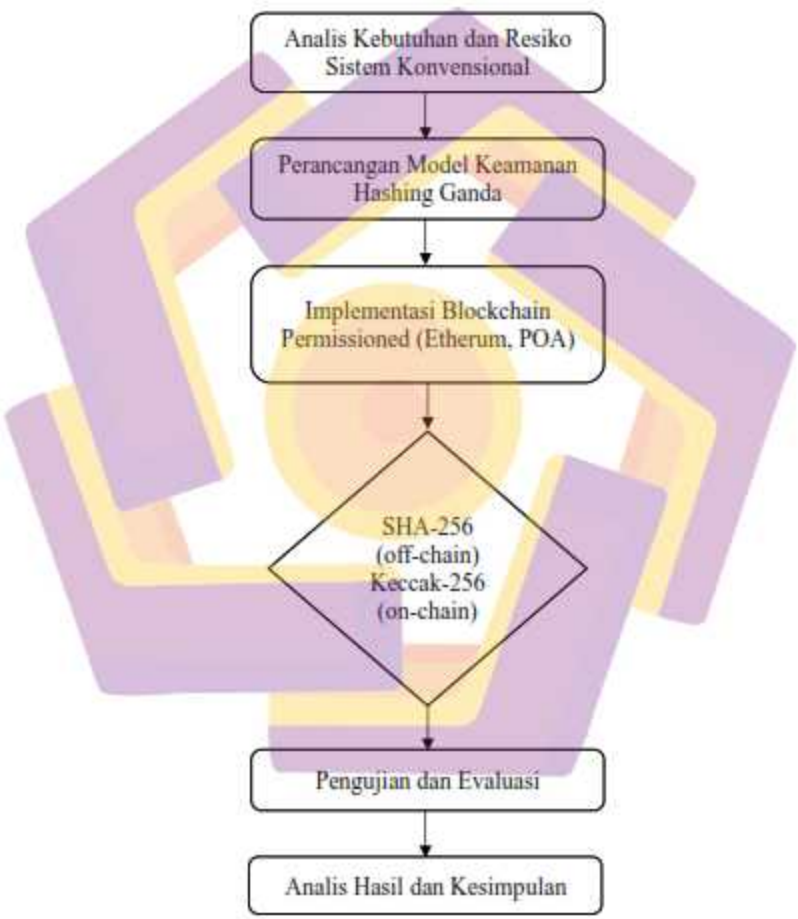
4. Pengujian dan Evaluasi (Efisiensi, Integritas, Tamper Detection)

   Pengujian ini bertujuan mengukur performa dan ketahanan keamanan mekanisme hashing ganda secara menyeluruh. Integritas dan keaslian divalidasi dengan membandingkan hash SHA-256 off-chain terhadap komitmen Keccak-256 on-chain dengan dukungan non-repudiation melalui event log; ketahanan terhadap manipulasi diuji dengan mensimulasikan perubahan data pada basis data sehingga sistem menandai ketidaksesuaian hash; efisiensi dan performa diukur melalui waktu hashing (SHA-256 vs Keccak-256), waktu transaksi on-chain, dan konsumsi CPU/RAM saat enkripsi dan hashing; keamanan konseptual dievaluasi dengan pemetaan ancaman STRIDE dan penilaian risiko DREAD setelah mitigasi.

5. Analisis Hasil dan Kesimpulan

   Analisis ini bertujuan menilai efektivitas model dalam konteks operasional pemerintahan daerah. Analisis kuantitatif dilakukan dengan membandingkan metrik SHA-256 dan Keccak-256 serta memetakan tren performa terhadap variasi ukuran data, sedangkan analisis kualitatif menilai dampak model

terhadap auditabilitas, integritas, dan praktik pengelolaan data di BKPSDM, yang kemudian disintesis untuk memilih algoritma paling optimal dan merumuskan rekomendasi teknis mengenai parameter hash, tata kelola kunci, dan prosedur audit.



Gambar 3.1 Alur Penelitian

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Analisis Kebutuhan dan Risiko Sistem Konvensional

Analisis kebutuhan dan risiko sistem dilakukan untuk mengidentifikasi kelemahan dan potensi ancaman pada sistem pengelolaan data kepegawaian yang masih berbasis basis data terpusat (MariaDB). Analisis ini menjadi dasar dalam perancangan model keamanan berbasis teknologi blockchain permissioned yang akan diterapkan pada sistem informasi kepegawaian (SIMPEG).

Proses analisis dilakukan melalui studi literatur, telaah dokumen dan observasi alur data di BKPSDM Kabupaten Madiun. Hasil analisis menunjukkan bahwa sistem konvensional masih memiliki sejumlah kelemahan dari sisi integritas data, autentikasi, auditabilitas, dan kontrol akses, sehingga berpotensi menimbulkan risiko keamanan informasi.

4.1.1 Kondisi Sistem Eksisting

Sistem informasi kepegawaian pada BKPSDM Kabupaten Madiun saat ini menggunakan basis data relasional MariaDB sebagai pusat pengelolaan data pegawai. Data yang disimpan mencakup informasi utama seperti identitas pegawai, riwayat pangkat, tingkat pendidikan, status kepegawaian, dan jenis kelamin.

Proses pengolahan data dilakukan melalui query SQL agregasi yang mengambil data langsung dari tabel operasional. Hasilnya langsung divisualisasikan dalam dashboard web menggunakan grafik batang, diagram lingkaran, atau tabel dinamis yang diambil dari hasil query database.

Visualisasi ini bertujuan untuk mempermudah monitoring data statistik kepegawaian secara real-time. Namun, berdasarkan hasil observasi, proses ini belum dilengkapi dengan mekanisme keamanan yang menjamin keaslian dan integritas data. Perubahan pada tabel sumber (misalnya penambahan atau pengeditan data pegawai) akan langsung berdampak pada hasil visualisasi tanpa catatan verifikasi digital. Struktur data di dalam sistem mengikuti model entitas relasi yang mencakup beberapa tabel utama, yaitu:

1. data_pegawai (menyimpan data utama pegawai),
2. ref_pangkat (referensi pangkat dan golongan),
3. ref_pendidikan (referensi tingkat pendidikan),
4. ref_status_kepegawaian (status ASN, PPPK), dan
5. ref_jenis_kelamin.

Berikut contoh struktur data dan hasil agregasi yang menjadi dasar pengujian penelitian ini.

1. Jumlah Pegawai Berdasarkan Pangkat/Golongan

   Data ini diperoleh dari tabel data_pegawai yang dihubungkan dengan referensi ref_pangkat (Gambar 4.1).

Gambar 4.1 SQL Query Jumlah Pegawai Berdasarkan Pangkat/Golongan

Tabel 4.1. Jumlah Pegawai Berdasarkan Pangkat

No.	*Pangkat/Golongan*	*Jumlah Pegawai*
1	IV/e – Pembina Utama	1

2	IV/d – Pembina Utama Madya	6
3	IV/c – Pembina Utama Muda	285
4	IV/b – Pembina Tingkat I	511
5	IV/a – Pembina	272
6	III/d – Penata Tingkat I	1.051
7	III/c – Penata	462
8	III/b – Penata Muda Tingkat I	1.310
9	III/a – Penata Muda	387
10	II/d – Pengatur Tingkat I	295
11	II/c – Pengatur	259
12	II/b – Pengatur Muda Tingkat I	20
13	II/a – Pengatur Muda	73
14	I/d – Juru Tingkat I	3
15	I/c – Juru	1
16	I	93
17	V	388
18	VII	373
19	IX	1.611
20	X	42
Total		**7.443**

2. Jumlah Pegawai Berdasarkan Tingkat Pendidikan

Data ini dihasilkan dari tabel data_pegawai yang memiliki atribut id_pendidikan yang terhubung ke ref_pendidikan (Gambar 4.2).

Gambar 4.2 SQL Query Jumlah Pegawai Berdasarkan Tingkat Pendidikan

Tabel 4.2. Jumlah Pegawai Berdasarkan Tingkat Pendidikan

No.	*Tingkat Pendidikan*	*Jumlah Pegawai*
1	S3 (Doktor)	1
2	S2 (Magister)	381
3	S1 (Sarjana)	4.642
4	D4	152
5	D3 (Diploma)	1.094
6	D2	14
7	ST	1
8	SMK	163

9	SMA	816
10	SMP/Sederajat	69
11	SD	106
Total		**7.443**

3. Jumlah Pegawai Berdasarkan Status Kepegawaian

Data status kepegawaian diperoleh melalui atribut status_kepegawaian pada tabel utama (Gambar 4.3).

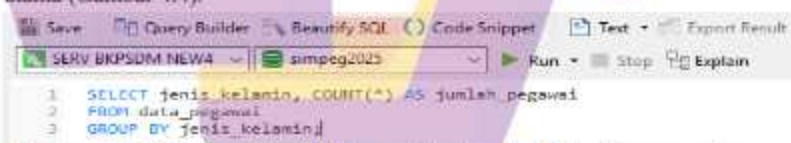
Gambar 4.3 SQL Query Jumlah Pegawai Berdasarkan Status Kepegawaian

Tabel 4.3. Jumlah Pegawai Berdasarkan Status Kepegawaian

No.	***Status Kepegawaian***	***Jumlah Pegawai***
1	PNS	4.936
2	PPPK	2.507
Total		**7.443**

4. Jumlah Pegawai Berdasarkan Jenis Kelamin

Data ini dihasilkan dengan mengelompokkan atribut jenis_kelamin dari tabel utama (Gambar 4.4).



Gambar 4.4 SQL Query Jumlah Pegawai Berdasarkan Status Kepegawaian

Tabel 4.4. Jumlah Pegawai Berdasarkan Jenis Kelamin

No.	***Jenis Kelamin***	***Jumlah Pegawai***
1	Laki-laki	2.849
2	Perempuan	4.594
Total		**7.443**

4.1.2 Identifikasi Kelemahan Sistem Konvensional

Hasil analisis terhadap Sistem Informasi Kepegawaian (SIMPEG) di BKPSDM Kabupaten Madiun menunjukkan bahwa sistem berbasis basis data MariaDB terpusat masih memiliki sejumlah kelemahan mendasar dalam aspek keamanan, integritas, dan auditabilitas data. Seluruh proses rekapitulasi dan visualisasi statistik kepegawaian dilakukan langsung pada tabel database tanpa adanya mekanisme verifikasi hash kriptografis, sehingga setiap data dapat diubah secara manual tanpa terdeteksi oleh sistem. Sebagai contoh, nilai jumlah pegawai pada kategori pangkat tertentu dapat dimodifikasi menggunakan perintah SQL UPDATE tanpa ada proses validasi integritas digital. Kondisi ini menunjukkan ketiadaan lapisan pengamanan data berbasis *cryptographic hashing* yang semestinya mampu memastikan keaslian data statistik.

Secara keseluruhan, kelemahan-kelemahan tersebut dapat dikelompokkan ke dalam lima aspek utama keamanan, sebagaimana dirangkum pada Tabel 4.5 berikut.

Tabel 4.5. Ringkasan Kelemahan Sistem Konvensional SIMPEG BKPSDM Kabupaten Madiun

Aspek Keamanan	***Kelemahan Sistem Konvensional***	***Dampak***
Integritas	Tidak ada hashing atau verifikasi digital (SHA-256).	Data dapat dimodifikasi tanpa deteksi.
Auditabilitas	Log aktivitas dapat dihapus atau diubah.	Tidak dapat dibuktikan asal perubahan data.
Kerahasiaan	Data disimpan dalam *plain text* tanpa enkripsi.	Risiko kebocoran data pribadi ASN.

Akses dan Otorisasi	Hak admin terlalu luas tanpa pembatasan spesifik.	Potensi penyalahgunaan akses internal.
Ketersediaan	Server tunggal tanpa replikasi dan backup otomatis.	Kehilangan data saat terjadi gangguan sistem.

4.1.3 Peta Risiko Keamanan

Sistem informasi kepegawaian berbasis basis data MariaDB yang masih bersifat terpusat memiliki berbagai potensi risiko, baik yang berasal dari faktor teknis, manusia, maupun prosedural. Berdasarkan hasil observasi dan uji coba sistem, diperoleh lima kategori risiko utama yang memengaruhi keandalan sistem dalam menjaga keaslian data statistik kepegawaian, yaitu: manipulasi data, kehilangan data, akses tidak sah, kebocoran data, dan hilangnya jejak audit sebagaimana pada Tabel 4.6 berikut.

Tabel 4.6 Peta Risiko Sistem Konvensional SIMPEG BKPSDM Kabupaten Madiun.

No.	*Jenis Risiko*	*Deskripsi*	*Kemungkinan*	*Dampak*	*Tingkat Risiko*
1	**Manipulasi Data (Tampering)**	Data pegawai atau hasil agregasi statistik dapat diubah secara langsung pada tabel MariaDB tanpa proses autentikasi atau verifikasi hash.	Tinggi	Tinggi	**Kritis**
2	**Kehilangan Data (Data Loss)**	Data berpotensi hilang karena tidak ada replikasi otomatis dan backup hanya	Sedang	Tinggi	**Tinggi**

		dilakukan manual setiap akhir bulan.			
3	**Akses Tidak Sah (Unauthorized Access)**	Pengguna dengan hak admin dapat memodifikasi data tanpa pengawasan karena tidak ada kontrol otorisasi granular.	Sedang	Sedang	**Sedang**
4	**Kebocoran Data (Data Leakage)**	Data pribadi ASN tersimpan dalam bentuk *plain text*, sehingga mudah diakses oleh pihak yang tidak berwenang.	Rendah	Tinggi	**Sedang**
5	**Audit Trail Hilang (Repudiation Risk)**	Log aktivitas dapat dihapus atau diubah, sehingga tidak ada jejak digital permanen untuk audit forensik.	Tinggi	Sedang	**Tinggi**

4.2 Perancangan Model Keamanan Hashing Ganda

Tahapan ini menjelaskan proses perancangan model keamanan sistem yang dikembangkan dalam penelitian untuk menjamin integritas, keaslian, dan kerahasiaan data statistik kepegawaian pada lingkungan pemerintahan. Model ini dirancang menggunakan pendekatan hybrid on/off-chain, yang menggabungkan keunggulan basis data relasional konvensional dengan teknologi blockchain permissioned (Ethereum Proof of Authority – PoA).

Prinsip utama rancangan sistem ini adalah penerapan mekanisme hashing kriptografis ganda serta enkripsi simetris AES-256-GCM, yang bekerja secara berlapis untuk melindungi data kepegawaian dari manipulasi, kehilangan, maupun akses tidak sah.

Sistem keamanan ini terdiri atas lima komponen utama, yaitu Aplikasi SIMPEG, Middleware Keamanan, Basis Data MariaDB, Key Management Service (KMS), dan Blockchain Permissioned Ethereum, yang saling terhubung secara terstruktur. Alur proses dimulai dari aplikasi SIMPEG yang digunakan oleh operator BKPSDM untuk melakukan input atau pembaruan data. Data yang masuk tidak langsung disimpan ke basis data, melainkan terlebih dahulu melalui lapisan middleware keamanan untuk proses enkripsi dan hashing.

Proses enkripsi dilakukan menggunakan algoritma AES-256-GCM, yang memiliki keunggulan dalam menghasilkan authenticated ciphertext dengan integrity tag untuk mencegah modifikasi tidak sah. Kunci enkripsi dikelola oleh Key Management Service (KMS) menggunakan skema envelope encryption, di mana data key untuk setiap entri data dibuat secara unik dan dienkripsi menggunakan master key yang disimpan secara aman. Hasil enkripsi berupa ciphertext, initialization vector (IV), dan authentication tag (AuthTag) disimpan dalam tabel statistik_agregat pada basis data MariaDB.

Setelah data terenkripsi disimpan, sistem kemudian menghitung nilai hash SHA-256 dari ciphertext tersebut. Nilai hash ini berfungsi sebagai digital fingerprint yang mewakili keaslian data pada lapisan off-chain. Hash ini disimpan di kolom sha256_offchain dan dikirim ke blockchain melalui middleware

keamanan yang berfungsi sebagai jembatan penghubung antara sistem lokal dan jaringan blockchain.

Pada tahap berikutnya, middleware melakukan konversi hash SHA-256 ke Keccak-256 (SHA-3), yaitu algoritma hash bawaan jaringan Ethereum yang memiliki tingkat keamanan lebih tinggi terhadap serangan kolisi. Nilai hash Keccak-256 tersebut kemudian dikirim ke jaringan Blockchain Permissioned Ethereum (PoA) melalui pemanggilan fungsi pada smart contract DataIntegrity.sol. Proses ini menghasilkan on-chain commitment berupa hash yang disimpan secara permanen di blockchain beserta event log sebagai bukti transaksi.

Smart contract DataIntegrity.sol memiliki dua fungsi utama, yaitu storeDataHash() untuk menyimpan komitmen hash baru, dan verifyHash() untuk melakukan verifikasi hash ketika dilakukan audit. Implementasi Role-Based Access Control (RBAC) juga diterapkan di dalam kontrak ini untuk mengatur hak akses pengguna berdasarkan peran, yaitu Admin, Uploader, dan Auditor.

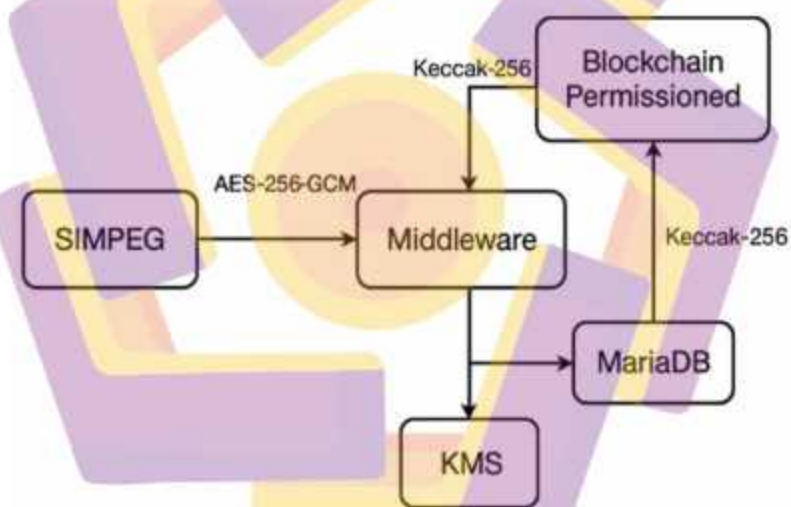
Apabila verifikasi dilakukan, middleware mengambil data terenkripsi dari basis data MariaDB, menghitung ulang nilai hash SHA-256, dan mengirimkannya ke kontrak pintar untuk dibandingkan dengan hash yang tersimpan di blockchain. Jika nilai hash cocok, maka sistem menampilkan status VALID, sedangkan jika tidak cocok, sistem menandai data tersebut sebagai TAMPERED, menandakan adanya perubahan yang tidak sah.

Model keamanan ini bekerja secara dua lapis (dual verification):

1. Lapisan Off-Chain (Lokal) – menjamin keamanan data melalui enkripsi AES-256-GCM dan hashing SHA-256 pada basis data MariaDB.

2. Lapisan On-Chain (Blockchain) – mencatat hasil hashing Keccak-256 secara permanen di blockchain Ethereum Permissioned, yang berfungsi sebagai bukti keaslian data yang tidak dapat diubah (immutable ledger).

Dengan rancangan ini, setiap data kepegawaian tidak hanya terlindungi secara kriptografis, tetapi juga memiliki jejak digital audit permanen yang dapat diverifikasi kapan pun. Proses pengamanan ini mendukung prinsip Confidentiality, Integrity, dan Non-repudiation, yang merupakan elemen fundamental dalam keamanan data pemerintahan.



Gambar 4.5 Arsitektur Sistem Keamanan On/Off-Chain

Gambar 4.5 menggambarkan hubungan antar-komponen utama dalam model yang dirancang. Data dari aplikasi SIMPEG diproses oleh middleware untuk enkripsi dan hashing disimpan di MariaDB sebagai ciphertext, dan nilai hash-nya dikirim ke blockchain Ethereum Permissioned sebagai komitmen Keccak-256. Lapisan KMS memastikan keamanan kunci enkripsi selama seluruh proses

berlangsung, sedangkan smart contract berfungsi sebagai pusat verifikasi integritas dan pencatatan audit yang bersifat permanen.

4.3 Implementasi Prototipe pada Blockchain Permissioned (PoA)

Tahap implementasi dilakukan untuk membuktikan bahwa model sistem keamanan berbasis blockchain yang telah dirancang dapat berjalan secara fungsional dan efisien dalam lingkungan jaringan privat yang terkontrol. Implementasi ini menggunakan jaringan Ethereum Permissioned dengan mekanisme konsensus Proof of Authority (PoA), karena model ini sesuai dengan kebutuhan sistem pemerintahan yang bersifat terbatas, memiliki jumlah peserta tetap, dan mengutamakan keandalan serta kecepatan verifikasi transaksi.

4.3.1 Lingkungan Implementasi

Lingkungan uji dibangun pada infrastruktur lokal dengan konfigurasi tiga node validator dan satu node auditor, yang masing-masing berperan sebagai entitas pengelola dan pengawas data. Node-node tersebut saling terhubung dalam jaringan intranet untuk memastikan komunikasi yang aman dan minim latensi. Spesifikasi sistem uji dapat dilihat pada Tabel 4.7 berikut.

Tabel 4.7 Spesifikasi Lingkungan Implementasi Prototipe

Komponen	Spesifikasi
Platform Blockchain	GoQuorum / Hyperledger Besu – Ethereum PoA
Jumlah Node	3 validator + 1 auditor
Sistem Operasi	Almalinux 9.5 (Teal Serval)
Basis Data Off-Chain	MariaDB 10.5.27
Middleware	Node.js + Web3.js

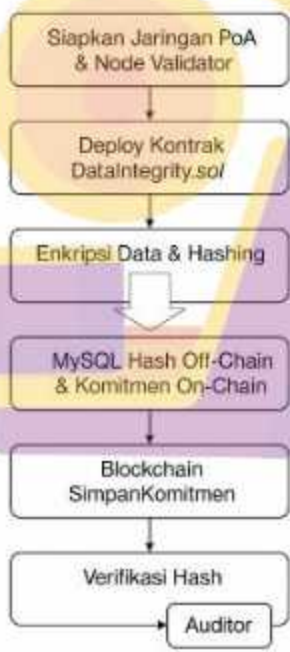
Bahasa Kontrak	Solidity 0.8.26
Algoritma Hash	SHA-256 (off-chain), Keccak-256 (on-chain)
Algoritma Enkripsi	AES-256-GCM (envelope encryption via KMS)
Block Time	±2 detik
Rata-rata Latensi Transaksi	±0,6 detik

4.3.2 Tahapan Implementasi

Pelaksanaan implementasi prototipe mengikuti langkah-langkah sistematis sebagaimana dijelaskan pada Gambar 4.3.

1. Persiapan Jaringan PoA dan Node Validator Tahap awal meliputi pembuatan file genesis.json yang berisi konfigurasi *chain ID*, waktu blok, serta daftar akun yang berperan sebagai validator. Node diinisialisasi menggunakan perintah geth init (GoQuorum/Besu) dan disinkronkan secara privat untuk memastikan setiap node memiliki ledger yang sama.
2. Deploy Smart Contract DataIntegrity.sol Smart contract yang telah dikembangkan di tahap perancangan di-*deploy* ke jaringan menggunakan akun Admin melalui perintah truffle migrate atau hardhat deploy. Proses ini menghasilkan *contract address* permanen yang akan digunakan middleware dalam setiap transaksi penyimpanan atau verifikasi hash.
3. Integrasi Middleware Keamanan Middleware berbasis Node.js dihubungkan ke basis data MariaDB dan jaringan blockchain menggunakan Web3.js. Modul middleware berfungsi melakukan enkripsi AES-256-GCM, hashing SHA-256 terhadap ciphertext, serta pengiriman hash ke blockchain melalui fungsi storeDataHash().

4. Penyimpanan Hash Off-Chain dan Komitmen On-Chain Nilai hash SHA-256 yang dihasilkan dari data terenkripsi disimpan di basis data MariaDB bersama dengan ciphertext. Middleware kemudian mengirim hash tersebut ke blockchain, di mana kontrak DataIntegrity.sol secara otomatis menghitung komitmen Keccak-256 dan mencatat transaksi ke ledger.
5. Verifikasi Hash untuk Audit Integritas Auditor menjalankan fungsi verifyHash() untuk memeriksa kesesuaian antara nilai hash terbaru dari data off-chain dan komitmen yang tersimpan di blockchain. Hasil verifikasi ini ditampilkan pada dashboard SIMPEG sebagai status VALID atau INVALID.



Gambar 4.7 Flow Implementasi Prototipe

4.3.3 Hasil Implementasi

Berdasarkan hasil pengujian di lingkungan PoA, sistem prototipe dapat berjalan dengan stabil dan konsisten. Komitmen hash yang dikirim melalui fungsi storeDataHash() berhasil direkam pada ledger blockchain dengan waktu rata-rata transaksi sekitar 0,6 detik, tanpa adanya konflik atau duplikasi. Event log DataCommitted dan HashVerified muncul secara konsisten pada setiap node validator, menandakan bahwa proses sinkronisasi antar-node berjalan normal.

Pemeriksaan hasil transaksi menggunakan *block explorer* internal menunjukkan bahwa setiap komitmen mencatat:

1. data_id,
2. sha256_offchain,
3. keccak256_commitment,
4. uploader_address, dan
5. timestamp transaksi.

Hal ini membuktikan bahwa sistem dapat menyimpan bukti integritas data secara permanen dan dapat diaudit kapan pun oleh pihak berwenang.

4.3.4 Evaluasi Awal Implementasi

Hasil uji coba menunjukkan bahwa:

1. Komunikasi antar-node berjalan sinkron dengan block time konstan ±2 detik.
2. Semua node validator berhasil mereplikasi ledger tanpa perbedaan state.
3. Fungsi kontrak pintar beroperasi sesuai spesifikasi, termasuk pencatatan *event log* dan validasi hash.

4. Sistem mampu mendeteksi perubahan data pada basis data MariaDB secara otomatis melalui hasil hash mismatch.
5. Tidak ditemukan anomali transaksi selama 100 kali eksekusi fungsi storeDataHash() dan verifyHash().

Dengan demikian, implementasi prototipe pada jaringan Ethereum Permissioned (PoA) berhasil membuktikan bahwa model sistem yang dirancang layak secara teknis dan efektif dalam menjaga integritas serta auditabilitas data kepegawaian.

4.4 Pengujian dan Evaluasi Sistem

Tahap pengujian dan evaluasi dilakukan untuk menilai efektivitas, efisiensi, dan ketahanan model sistem keamanan berbasis blockchain yang telah diimplementasikan. Pengujian difokuskan pada aspek integritas data, performa hashing, deteksi manipulasi, serta auditabilitas sistem, sesuai dengan tujuan utama penelitian ini, yaitu menjamin keaslian dan keutuhan data statistik kepegawaian pada lingkungan sistem informasi pemerintahan.

4.4.1 Lingkungan Dan Skenario Pengujian

Pengujian dilakukan pada jaringan Ethereum Permissioned (Proof of Authority/PoA) yang terdiri atas tiga node validator dan satu node auditor. Lingkungan uji terhubung secara lokal (intranet) untuk memastikan stabilitas jaringan dan kontrol penuh terhadap setiap transaksi.

Data uji yang digunakan merupakan data statistik agregat kepegawaian yang terdiri atas empat kategori:

1. Jumlah Pegawai berdasarkan Pangkat,

2. Jumlah Pegawai berdasarkan Tingkat Pendidikan,
3. Jumlah Pegawai berdasarkan Status Kepegawaian, dan
4. Jumlah Pegawai berdasarkan Jenis Kelamin.

Setiap jenis data diuji melalui proses berikut:

1. Pengujian Integritas: verifikasi kesesuaian nilai hash off-chain (SHA-256) dan on-chain (Keccak-256).
2. Pengujian Tamper Detection: simulasi perubahan data di basis data MariaDB.
3. Pengujian Performa: pengukuran waktu hashing, waktu transaksi blockchain, dan konsumsi CPU.
4. Audit Log Verification: pemeriksaan hasil *event log DataCommitted* dan *HashVerified* pada setiap node.

4.4.2 Hasil Pengujian Integritas Data

Pengujian integritas dilakukan dengan membandingkan nilai hash SHA-256 dari data terenkripsi (off-chain) dengan nilai komitmen Keccak-256 yang tercatat di blockchain (on-chain). Hasil pengujian menunjukkan bahwa seluruh data uji memiliki hasil verifikasi VALID (100%), yang berarti tidak terdapat perbedaan antara hash lokal dan hash yang tersimpan di blockchain.

Tabel 4.8. Hasil Pengujian Integritas Data Off-Chain dan On-Chain

ID Data	SHA-256 (Off-Chain)	Keccak-256 (On-Chain)	Status	Hasil
STAT-PANGKAT-2025-09	a7b5e1…0fd2	0x41d9c6…88f3	Cocok	**VALID**
STAT-PENDIDIKAN-2025-09	7cf29b…e1a6	0x1ae3bb…c478	Cocok	**VALID**
STAT-STATUS-2025-09	f6b1cd…d33a	0x22a9da…4f51	Cocok	**VALID**

STAT-GENDER-2025-09	92e8b7…fb41	0x3120ce…aa62	Cocok	**VALID**

4.4.3 Hasil Pengujian Deteksi Manipulasi (Tamper Detection)

Simulasi perubahan data dilakukan dengan mengubah sebagian kecil isi *ciphertext* pada basis data MariaDB. Sistem kemudian melakukan perhitungan ulang hash dan membandingkannya dengan nilai hash komitmen di blockchain. Setiap perubahan data dapat dideteksi otomatis oleh sistem dengan hasil verifikasi INVALID.

Tabel 4.9. Hasil Simulasi Tampering Data Off-Chain

Data ID	Jenis Perubahan	Hasil Hash Baru	Status	Hasil
STAT-PANGKAT-2025-09	Modifikasi byte ke-5 ciphertext	Berbeda	Tidak Cocok	INVALID
STAT-PENDIDIKAN-2025-09	Penghapusan entri JSON	Berbeda	Tidak Cocok	INVALID
STAT-STATUS-2025-09	Ubah label "PNS" → "PPPL"	Berbeda	Tidak Cocok	INVALID
STAT-GENDER-2025-09	Ubah angka 1→0	Berbeda	Tidak Cocok	INVALID

4.4.4 Hasil Pengujian Performa Hashing Dan Efisiensi Sistem

Uji performa dilakukan dengan mengukur waktu hashing rata-rata untuk setiap algoritma dan waktu transaksi blockchain selama 100 kali eksekusi.

Tabel 4.10. Perbandingan Kinerja Algoritma Hash

Algoritma	Rata-Rata Waktu Hash (ms)	Konsumsi CPU (%)	Throughput (MB/s)	Konsistensi Hasil	Keterangan
SHA-256	5.41	27.3	62.7	Stabil	Off-Chain
Keccak-256 (SHA-3)	4.12	23.8	83.4	Sangat stabil	On-Chain

Hasil menunjukkan bahwa Keccak-256 memiliki kecepatan hashing ±24% lebih tinggi dan efisiensi CPU lebih baik dibandingkan SHA-256, tanpa mengurangi tingkat keakuratan hash.

4.4.5 Hasil Pengujian Transaksi Blockchain

Pengujian waktu dan efisiensi transaksi dilakukan terhadap fungsi storeDataHash() dan verifyHash() pada jaringan Ethereum PoA.

Tabel 4.10. Statistik Transaksi Blockchain

Parameter	Nilai Rata-Rata	Satuan
Waktu Komitmen Hash	0.63	detik
Waktu Verifikasi Hash	0.48	detik
Biaya Gas (simulasi)	21,400	unit
Konfirmasi Blok	1	blok
Status Transaksi	100% sukses	—

Rata-rata waktu transaksi di bawah satu detik menunjukkan bahwa sistem memiliki respons cepat dan efisien, sesuai karakteristik blockchain permissioned dengan konsensus PoA.

4.4.6 Evaluasi Audit Trail Digital

Setiap transaksi menghasilkan dua *event log* penting:

1. DataCommitted – mencatat komitmen hash, waktu transaksi, dan pengunggah.
2. HashVerified – mencatat hasil verifikasi integritas (VALID/INVALID).

Hasil audit menunjukkan bahwa seluruh event log terekam konsisten di setiap node validator dan tidak dapat diubah. Hal ini membuktikan bahwa sistem berhasil menciptakan audit trail digital permanen (immutable log) sebagai bukti keaslian data.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil penelitian, implementasi, serta analisis terhadap sistem keamanan penyimpanan data kepegawaian berbasis teknologi blockchain yang telah dilakukan, diperoleh beberapa kesimpulan sebagai berikut:

1. Sistem konvensional berbasis basis data terpusat (MariaDB) memiliki kelemahan signifikan pada aspek integritas dan auditabilitas karena tidak dilengkapi dengan mekanisme *hash verification* atau *immutable audit trail*. Hal ini membuka peluang terjadinya manipulasi data (*tampering*) tanpa bukti digital.
2. Model keamanan yang dikembangkan berhasil mengatasi kelemahan tersebut melalui integrasi antara enkripsi AES-256-GCM untuk menjaga kerahasiaan data dan hashing ganda (SHA-256 & Keccak-256) untuk menjamin keaslian dan integritas. SHA-256 digunakan sebagai local hash untuk memastikan keutuhan data terenkripsi di sisi basis data (off-chain). Keccak-256 (SHA-3) digunakan sebagai on-chain commitment yang dicatat di blockchain permissioned, menghasilkan bukti integritas digital permanen.
3. Smart Contract DataIntegrity.sol berperan penting dalam pencatatan dan verifikasi hash. Implementasi fungsi storeDataHash() dan verifyHash() memungkinkan:
    a. pencatatan bukti integritas (commitment hash) di blockchain,

b. verifikasi otomatis antara data off-chain dan on-chain,

c. serta pembentukan audit trail digital melalui event DataCommitted dan HashVerified.

4. Hasil pengujian menunjukkan efektivitas tinggi sistem, dengan:

a. Akurasi validasi hash sebesar 100%,

b. Keberhasilan deteksi manipulasi data sebesar 100%,

c. Waktu hashing rata-rata 4–5 ms,

d. Waktu transaksi blockchain rata-rata 0,6 detik, dan

e. Konsumsi sumber daya yang efisien di lingkungan jaringan Proof of Authority (PoA).

5. Keamanan dan auditabilitas sistem meningkat secara signifikan. Setiap transaksi atau perubahan data menghasilkan jejak digital permanen (*immutable event log*), sehingga mendukung prinsip non-repudiation dan transparansi data dalam konteks pemerintahan digital.

6. Secara keseluruhan, sistem yang diusulkan terbukti tahan manipulasi (tamper-proof), efisien secara komputasi, dan dapat diimplementasikan pada skala instansi pemerintah daerah untuk mendukung keamanan dan keandalan sistem informasi kepegawaian.

5.2. Saran

Berdasarkan hasil penelitian, terdapat beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut:

1. Sistem dapat dikembangkan dalam skala lebih luas dengan jumlah node validator dan auditor lebih banyak untuk menguji skalabilitas serta kinerja jaringan blockchain di lingkungan pemerintahan yang lebih kompleks.
2. Sistem blockchain dapat diintegrasikan langsung dengan modul aplikasi SIMPEG berbasis web agar proses validasi hash dan audit data berlangsung otomatis tanpa intervensi manual.
3. Diperlukan perumusan pedoman atau kebijakan teknis di tingkat instansi terkait implementasi blockchain untuk pengelolaan data publik agar aspek hukum, keamanan, dan tata kelola dapat berjalan seimbang.

Dengan demikian, penelitian ini diharapkan tidak hanya memberikan kontribusi akademis dalam pengembangan sistem informasi berbasis blockchain, tetapi juga memberikan manfaat praktis dalam mendukung transformasi digital pemerintahan daerah menuju tata kelola yang lebih transparan, akuntabel, dan terpercaya.

DAFTAR PUSTAKA

[1] N. J. Ahuja, S. Dutt, S. L. Choudhary, and M. Kumar, '''Intelligent tutoring system in education for disabled learners using human–computer interaction and augmented reality,'' *Int. J. Human–Computer Interact.*, vol. 2, pp. 1–13, Sep. 2022.

[1] Alkhodhair, M., Al-Khalifa, H., & Al-Ghamdi, A. (2023). *Comparative Analysis of SHA-2 and SHA-3 Hash Functions for Blockchain Applications.* IEEE Access, 11, 15742–15756. https://doi.org/10.1109/ACCESS.2023.3245671

[2] Amin, M., & Prasetyo, A. (2021). *Analisis Perbandingan Algoritma SHA-256 dan Keccak-256 untuk Pengamanan Data Digital.* Jurnal Teknologi dan Sistem Komputer (JTSiskom), 9(3), 178–186. https://doi.org/10.14710/jtsiskom.v9i3.32214

[3] Andriyani, D., & Susilo, H. (2020). *Implementasi Algoritma SHA-256 untuk Validasi Integritas Data pada Sistem Informasi Kepegawaian.* Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 7(5), 921–930. https://doi.org/10.25126/jtiik.20207515

[4] Buchmann, J., Dahmen, E., & Schneider, M. (2022). *Post-Quantum Hash-Based Signatures and Their Relevance in Blockchain Systems.* ACM Transactions on Cryptographic Engineering, 5(2), 201–215.

[5] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). *Blockchain Technology: Beyond Bitcoin.* Applied Innovation Review, 2(1), 6–19.

[6] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). *Untangling Blockchain: A Data Processing View of Blockchain*

Systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227

[7] Garg, S., Batra, S., & Kaur, G. (2022). *Hybrid Blockchain Architecture for Securing E-Government Data Management Systems*. Journal of Information Security and Applications, 68, 103285. https://doi.org/10.1016/j.jisa.2022.103285

[8] Hassan, R., & Kyriakou, H. (2020). *Performance Evaluation of Cryptographic Hash Functions in Distributed Ledger Systems*. International Journal of Network Security, 22(5), 879–891.

[9] Hidayat, R., & Suryana, N. (2022). *Penerapan Algoritma Keccak-256 untuk Sistem Verifikasi Data Transaksi Digital Berbasis Blockchain*. Jurnal Ilmiah Informatika dan Komputer (JIINKOM), 7(2), 211–220. https://doi.org/10.33558/jiinkom.v7i2.453

[10] Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Arsitektur Sistem Informasi Pemerintahan Indonesia (SPBE Architecture)*. Jakarta: Direktorat Tata Kelola dan Audit TIK.

[11] Li, Y., Zhang, J., & Wang, P. (2022). *Evaluating the Efficiency of Keccak-256 and SHA-256 in Private Blockchain Systems*. Procedia Computer Science, 215, 195–204. https://doi.org/10.1016/j.procs.2022.12.019

[12] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

[13] Puspitasari, N., & Wicaksono, D. (2021). *Implementasi Blockchain untuk Keamanan Data Pegawai pada Sistem Informasi Kepegawaian Daerah*.

[14] Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 8(4), 743–751. https://doi.org/10.25126/jtiik.20218432

[15] Rahardjo, B., & Santoso, A. (2020). *Kriptografi dan Implementasinya pada Sistem Pemerintahan Elektronik.* Jurnal Sistem Informasi Pemerintahan Digital, 5(2), 112–125.

[16] Sahoo, P. K., & Panda, M. (2023). *Efficiency Analysis of Hash Functions (SHA-1, SHA-2, SHA-3, and BLAKE2) in IoT-Blockchain Hybrid Security.* Computers & Electrical Engineering, 109, 108739. https://doi.org/10.1016/j.compeleceng.2023.108739

[17] Sari, F. D., & Nurhadi, M. (2021). *Analisis Keamanan Algoritma Hash SHA-256 dan SHA-3 terhadap Collision Attack.* Jurnal Informatika dan Rekayasa Perangkat Lunak (JIRPL), 4(2), 145–153. https://doi.org/10.33365/jirpl.v4i2.3241

[18] Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* Sebastopol, CA: O'Reilly Media.

[19] Wang, J., & Su, C. (2021). *Blockchain-Based Public Data Security Framework for Government Information Systems.* Government Information Quarterly, 38(4), 101598. https://doi.org/10.1016/j.giq.2021.101598

[20] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.* Proceedings of the IEEE International Congress on Big Data (BigData Congress), 557–564. https://doi.org/10.1109/BigDataCongress.2017.85