

**RANCANG BANGUN *PRIVATE STORAGE* BERBASIS
KONTAINERISASI DENGAN *AUDIT LOG BLOCKCHAIN*
(studi kasus : XYZ)**

PROPOSAL SKRIPSI



Disusun oleh:

Zulfan Farikh Rizano

(231011700464)

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PAMULANG
TANGERANG SELATAN
2026**

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan hidayah-Nya, sehingga proposal skripsi skripsi berjudul “RANCANG BANGUN *PRIVATE STORAGE* BERBASIS KONTAINERISASI DENGAN *AUDIT LOG BLOCKCHAIN* (studi kasus : XYZ) “ ini dapat diselesaikan dengan baik. Proposal skripsi ini disusun untuk memenuhi salah satu syarat akademis pada Program Studi Sistem Informasi (S1) Universitas Pamulang. Penulis menyadari bahwa keberhasilan proposal skripsi tidak lepas dari dukungan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Dr. Pranoto, S.E., M.M., selaku Ketua Yayasan Sasmita Jaya yang telah memfasilitasi sarana pendidikan di Universitas Pamulang dengan biaya terjangkau.
2. Dr. E. Nurzaman, A.M., M.M., M.Si., selaku Rektor Universitas Pamulang atas motivasi belajar yang diberikan kepada mahasiswa.
3. Bapak Heri Haerudin, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi Universitas Pamulang atas arahan programnya.
4. Ibu Annah Juliana, S.T., M.Kom., selaku Dosen Pembimbing atas bimbingan dan masukan berharganya.

Penulis menyadari proposal skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan. Semoga proposal skripsi ini dapat memberikan manfaat bagi perkembangan ilmu Sistem Informasi.

Tangerang Selatan, 03 September 2026

Zulfan Farikh Rizano

DAFTAR ISI

KATA PENGANTAR	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	vi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	3
1.4 Batasan Masalah.....	4
1.5 Tujuan Penelitian.....	5
1.6 Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA	6
2.1. Penelitian Terdahulu	6
2.2. Landasan Teori	10
2.2.1 Konsep <i>Cloud Storage</i> dan Keamanan Berkas	10
2.2.2 <i>Object Storage</i> MinIO dan Virtualisasi Server	11
2.2.3 <i>Private Blockchain</i> dan Konsensus Internal	11
2.2.4 Algoritma SHA-256 dan Skema <i>Hash-Chaining</i>	12
2.2.5 Kontainerisasi <i>Docker</i> dan Arsitektur <i>Microservices</i>	13
2.2.6 Otentikasi JSON <i>Web Token</i> (JWT) dan <i>Role-Based Access Control</i> (RBAC).....	14
2.2.7 Aksesibilitas Terenkripsi Menggunakan <i>Cloudflare Tunnel</i> (<i>Zero Trust</i>)...	14
2.3. Kerangka Berfikir	15
BAB III METODE PENELITIAN	16
3.1. Analisis Kebutuhan	16
3.1.1 Kebutuhan Fungsional (<i>Functional Requirements</i>).....	16

3.1.2 Kebutuhan Non-Fungsional (<i>Non-Functional Requirements</i>).....	17
3.2. Metode Penelitian.....	18
3.3. Metode Pengembangan Sistem	18
3.3.1 Kerangka Penelitian (NDLC)	18
3.3.2 Arsitektur dan Spesifikasi Teknis	19
3.4. Jadwal Penelitian	20
DAFTAR PUSTAKA	22

DAFTAR GAMBAR

Gambar 2. 1 Kerangka Berfikir.....	15
------------------------------------	----

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	6
Tabel 2. 2 Algoritma SHA-256	13
Tabel 3. 1 Jadwal Penelitian.....	20

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengelolaan administrasi dokumen akademik di lingkungan Sekolah Menengah Kejuruan (SMK) saat ini menuntut keterandalan sistem yang mampu menjamin keamanan serta kecepatan akses data. Berkas seperti ijazah kelulusan dan laporan Kerja Praktik (PKL) bukan sekadar arsip rutin sekolah, melainkan dokumen legal yang krusial bagi alumni untuk melanjutkan studi maupun melamar pekerjaan (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024). Oleh sebab itu, integritas data serta kemudahan proses verifikasi keabsahan dokumen tersebut menjadi hal esensial yang harus dipenuhi oleh pihak sekolah (Swastika dkk., 2022).

Kendati demikian, proses pengarsipan di SMK XYZ masih dihadapkan pada kendala klasik. Penyimpanan dokumen yang masih dilakukan secara semi-manual dan tersebar di beberapa unit kerja seperti Tata Usaha dan Program Keahlian menciptakan risiko kehilangan serta kerusakan fisik berkas. Selain itu, kondisi ini berdampak langsung pada lambatnya proses pencarian dokumen ketika alumni memerlukan legalisir atau penelusuran rekam data lama (Rawul dkk., 2025).

Masalah lain muncul pada alur verifikasi keaslian dokumen (Abidin & Munggaran, 2025). Pihak luar seperti instansi perusahaan atau perguruan tinggi umumnya masih mengandalkan mekanisme konvensional, di mana alumni diwajibkan datang langsung ke sekolah untuk menunjukkan fisik ijazah dan meminta cap legalisasi. Prosedur ini tidak efisien dari segi waktu dan biaya, serta menyimpan celah keamanan karena tidak adanya sarana verifikasi digital terpusat yang memadai untuk mencegah pemalsuan berkas (Abidin & Munggaran, 2025; Zulkarnain & Amien, 2025).

Dari sisi teknis pengelolaan server lokal, sistem basis data konvensional memiliki kelemahan mendasar pada perlindungan catatan aktivitas (*audit log*). Rekam aktivitas pada basis data relasional standar terhitung rentan dimodifikasi oleh oknum yang menguasai hak akses tingkat administrator (Pratama & Setiawan, 2024). Tanpa adanya perlindungan khusus, tindakan pengubahan atau penghapusan log dapat dilakukan tanpa meninggalkan jejak (Almotawkel & Obaid, 2026).

Di samping isu keamanan data, efisiensi penggunaan perangkat keras server sekolah juga menjadi perhatian tersendiri (Nugroho & Santoso, 2023). Penggunaan *Virtual Machine* (VM) tradisional untuk mengisolasi setiap modul aplikasi sering kali membebankan kinerja CPU dan RAM secara berlebihan. Pendekatan arsitektur *microservice* dan kontainerisasi dapat menjadi alternatif tepat karena mampu menjalankan beberapa layanan secara terisolasi dengan menghemat konsumsi sumber daya fisik server (Rahmatulloh dkk., 2025).

Untuk memberikan akses *remote* dari luar jaringan server lokal, penggunaan jalur koneksi terenkripsi yang efisien sangat dibutuhkan agar terhindar dari ancaman keamanan jaringan (Hidra Amnur & Putri, 2025). Akses eksternal yang aman memungkinkan pengujian dan verifikasi dilakukan dari jarak jauh tanpa perlu mengekspos infrastruktur jaringan internal sekolah secara terbuka. Sementara itu, guna memastikan berkas digital tidak dapat dimanipulasi (*immutable*), penerapan konsep *blockchain* menawarkan mekanisme validasi yang presisi (Kang dkk., 2022). Setiap dokumen dan *audit log* diikat menggunakan fungsi *kriptografi*, sehingga setiap bentuk perubahan ilegal pada berkas akan secara otomatis terdeteksi (Abidin & Munggaran, 2025; Zulkarnain & Amien, 2025).

Berdasarkan paparan permasalahan di atas, penelitian ini diarahkan untuk menyusun laporan dengan judul "RANCANG BANGUN *PRIVATE STORAGE* BERBASIS KONTAINERISASI DENGAN *AUDIT LOG BLOCKCHAIN* (studi kasus : XYZ)".

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang penulis uraikan di atas, maka identifikasi masalah dalam penelitian ini adalah sebagai berikut:

- a. Pengarsipan ijazah dan laporan PKL alumni di SMK XYZ masih berjalan secara semi-manual serta tersebar di berbagai unit kerja, sehingga rawan mengalami kerusakan, kehilangan, atau penyusutan efisiensi penelusuran data.
- b. Verifikasi dan legalisir ijazah masih mengharuskan kehadiran fisik alumni di sekolah akibat belum tersedianya platform verifikasi digital terpusat yang dapat diakses publik secara tepercaya.
- c. Belum tersedianya skema otentikasi keaslian dokumen secara otomatis untuk mendeteksi tindakan pemalsuan atau manipulasi pada berkas ijazah maupun laporan PKL.
- d. Catatan *audit log* pada sistem penyimpanan konvensional rentan diubah atau dihapus oleh oknum pemilik hak akses server guna menyembunyikan rekam aktivitas.
- e. Penggunaan sumber daya server berpotensi tidak efisien apabila setiap modul aplikasi dipaksa berjalan di atas mesin Virtual terpisah tanpa teknik kontainerisasi.
- f. Adanya potensi ancaman keamanan jaringan lokal sekolah jika akses eksternal dilakukan melalui pembukaan port publik router secara langsung.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang penulis uraikan di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

- a. Bagaimana mengimplementasikan arsitektur *Private Cloud Storage* berbasis *Docker Container* di atas *VMware Ubuntu Server* yang efisien untuk menyimpan ijazah dan laporan PKL pada SMK XYZ?
- b. Bagaimana merancang skema *audit log* berbasis *hash-chain blockchain* dan otentikasi JWT agar keaslian ijazah dan laporan PKL dapat diverifikasi serta manipulasi data dapat terdeteksi secara otomatis?

- c. Bagaimana menerapkan kontrol akses berbasis 3 aktor (Administrator, Pengguna, Auditor) serta aksesibilitas jaringan eksternal yang aman menggunakan *Cloudflare Tunnel*, sehingga proses verifikasi keaslian dokumen dapat dilakukan tanpa mengunjungi sekolah secara langsung?

1.4 Batasan Masalah

Berdasarkan latar belakang yang penulis uraikan di atas, maka batasan masalah dalam penelitian ini adalah sebagai berikut

- a. Lingkungan server dibangun pada sistem operasi Ubuntu Server 22.04 LTS yang berjalan di atas *hypervisor VMware Workstation Pro*, dengan penyimpanan data fisik terpisah pada partisi HDD (/mnt/cloud-storage).
- b. Implementasi kontainer menggunakan *Docker Compose* yang membungkus 3 service utama: *storage-service* (MinIO), *blockchain-service* (*Flask API & MySQL DB*), dan *dashboard-Web* (Nginx dengan tiga *dashboard custom*).
- c. Basis data relasional menggunakan MySQL dengan 7 tabel operasional (folders, files, file_versions, file_permissions, audit_logs, integrity_records) ditambah 1 tabel pengguna (users).
- d. Skema *blockchain* yang diterapkan berjenis *Private hash-chain* satu *Node* (*single-Node*) terpusat yang difokuskan untuk pendeteksian *tampering* log lokal bukan jaringan *blockchain* publik terdesentralisasi.
- e. Pembagian hak akses (RBAC) dibatasi pada 3 aktor: Administrator (kelola user, unggah, unduh, hapus berkas, *audit log*), Pengguna (unggah laporan PKL, unduh berkas sesuai izin), dan Auditor (verifikasi integritas dokumen, pemantauan *audit log*).
- f. Objek dokumen yang dikelola difokuskan pada dua jenis berkas digital: ijazah dan laporan PKL siswa berformat PDF.
- g. Akses eksternal memanfaatkan jalur terenkripsi HTTPS melalui *Cloudflare Tunnel* tanpa melakukan *port forwarding* pada router sekolah.

1.5 Tujuan Penelitian

Berdasarkan latar belakang yang penulis uraikan di atas, maka tujuan penelitian dalam penelitian ini adalah sebagai berikut

- a. Membangun infrastruktur *Private Cloud Storage* berbasis kontainer *Docker* yang efisien dalam menghemat penggunaan sumber daya server untuk menyimpan arsip ijazah dan laporan PKL di SMK XYZ.
- b. Membangun modul *audit log* berbasis *blockchain* guna menjamin keabsahan dokumen serta mendeteksi adanya perubahan berkas secara otomatis.
- c. Mengimplementasikan antarmuka *custom dashboard* dengan pembagian 3 aktor dan akses remote aman via *Cloudflare Tunnel* agar verifikasi keaslian dokumen dapat dilakukan dari jarak jauh.

1.6 Manfaat Penelitian

Berdasarkan latar belakang yang penulis uraikan di atas, maka identifikasi masalah dalam penelitian ini adalah sebagai berikut

- a. Manfaat Teoritis: Menjadi referensi akademis mengenai penerapan kontainerisasi aplikasi, *secure storage gateway*, serta validasi *blockchain* pada sistem pengarsipan dokumen di instansi pendidikan.
- b. Manfaat Praktis:
 - 1) Bagi Sekolah: Menghadirkan infrastruktur penyimpanan privat yang hemat sumber daya, mandiri, serta memiliki rekam aktivitas digital yang transparan dan aman dari modifikasi.
 - 2) Bagi Alumni: Mempermudah proses verifikasi keaslian ijazah oleh pihak luar (perusahaan atau perguruan tinggi) tanpa perlu hadir secara fisik di sekolah.
 - 3) Bagi Guru Pembimbing PKL: Menyediakan mekanisme pengarsipan laporan PKL siswa agar terpusat, rapi, dan mudah diaudit.

BAB II TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian mengenai tata kelola penyimpanan data, pengamanan transaksi digital, hingga pemanfaatan teknologi kontainerisasi dan *blockchain* telah berkembang pesat dalam beberapa tahun terakhir. Untuk memetakan posisi penelitian ini di tengah perkembangan keilmuan yang ada, dilakukan penelusuran terhadap 10 literatur relevan.

Tabel 2. 1 Penelitian Terdahulu

No	Penulis	Tahun	Judul Penelitian	Fokus Utama	Kekurangan / Celah Penelitian (Research Gap)	Peran & Kebaruan Penelitian Ini (Novelty)
1	Abidin & Munggaran	2025	<i>Blockchain-Based Digital Document Verification Using SHA-256 on the Internet Computer Protocol (ICP)</i>	Verifikasi keaslian dokumen digital menggunakan enkripsi SHA-256 yang ditanamkan pada platform <i>public/ICP blockchain</i> .	Mengandalkan <i>network public blockchain</i> (ICP) yang memerlukan biaya <i>gas fee</i> /token dan belum menangani penyimpanan fisik berkas besar secara privat (<i>on-premise</i>).	Menerapkan <i>audit log</i> pada <i>Private Blockchain</i> 1-Node untuk mencatat transaksi <i>hashing</i> tanpa biaya <i>gas fee</i> , terintegrasi langsung dengan penyimpanan MinIO.
2	Almotawkel & Obaid	2026	<i>Balancing Secrecy and Transparency in Smart Cities: a Systematic</i>	Tinjauan sistematis penyediaan kerahasia	Berupa studi literatur/konseptual, belum menyajikan rancangan arsitektur	Mengimplementasikan solusi praktis berupa arsitektur <i>PRIVATE STORAGE</i>

			<i>Review of Blockchain-Based Government Data Management</i>	an dan transparansi tata kelola data pemerintah berbasis <i>blockchain</i> .	<i>deployment</i> infrastruktur jaringan privat (<i>hybrid cloud/tunneling</i>).	berkinerja tinggi yang aman diakses dari mana saja melalui <i>Cloudflare Tunnel</i> .
3	Oktaviani & Pramudyo	2020	<i>Literature Review: Preservasi Penyimpanan Arsip Elektronik dalam Keamanan Arsip Menggunakan Teknologi Blockchain</i>	Analisis preservasi dan perlindungan integritas arsip elektronik melalui karakteristik <i>immutability</i> (anti-manipulasi) <i>blockchain</i> .	Belum mengimplementasikan sistem penyimpanan secara riil (masih sebatas <i>literature review</i>) serta tidak membahas arsitektur kontainerisasi.	Merancang dan mengimplementasikan sistem nyata berbasis <i>Docker Containerization</i> di atas Ubuntu Server (<i>VMware</i>) yang siap pakai.
4	Amnur & Putri	2025	<i>Zerotier Pada Home Server Menggunakan Sistem Operasi CasaOS</i>	Konfigurasi <i>home server</i> privat menggunakan CasaOS dan jaringan Virtual ZeroTier agar dapat diakses publik dengan aman.	Fokus hanya pada akses jaringan privat (<i>networking</i>), belum dilengkapi sistem <i>object storage enterprise</i> dan <i>audit log</i> berbasis <i>blockchain</i> untuk integritas data.	Menghubungkan <i>storage server</i> menggunakan <i>Cloudflare Tunnel</i> serta mengintegrasikan penyimpanan MinIO S3-compatible yang terverifikasi log <i>blockchain</i> .

5	Kang dkk.	2022	<i>Blockchain Private File Storage-Sharing Method Based on IPFS</i>	Berbagi file privat menggunakan gabungan IPFS (<i>InterPlanetary File System</i>) dan <i>blockchain</i> .	IPFS memiliki tantangan latensi dan kompleksitas <i>peer-to-peer</i> (P2P) jika diterapkan pada skala internal perusahaan/instansi.	Mengganti IPFS dengan MinIO Object Storage berbasis <i>S3 API</i> yang jauh lebih cepat untuk lingkungan lokal/Private server dengan <i>audit trail blockchain</i> .
6	Noman & Gwenhuire	2025	<i>Factors Influencing the Diffusion of Blockchain Technology in the Indonesian Government</i>	Analisis faktor-faktor yang mempengaruhi adopsi dan penyebaran teknologi <i>blockchain</i> di sektor pemerintahan Indonesia.	Berfokus pada analisis adopsi teknis dan organisasi (perspektif manajerial/kebijakan), belum memberikan model teknis implementasi <i>Private storage</i> .	Menyediakan acuan arsitektur teknis konkret (<i>proof of concept</i>) penerapan <i>blockchain Private 1-Node</i> yang hemat biaya dan siap diadopsi instansi lokal/terbatas.
7	Rahmatulloh dkk.	2025	<i>Arsitektur Microservice untuk Optimalisasi Aplikasi Eco-Maps dalam Mendukung Kampus Ramah Lingkungan</i>	Penerapan arsitektur <i>Microservices</i> menggunakan kontainerisasi untuk modularitas dan	Berfokus pada arsitektur perangkat lunak <i>Microservices</i> umum, tanpa mekanisme validasi keamanan/ <i>audit log immutable</i> pada	Memanfaatkan <i>Docker</i> untuk kontainerisasi layanan <i>storage</i> (MinIO, <i>Node Blockchain</i> , Tunnel) sekaligus menjamin keabsahan <i>log access</i> via <i>blockchain</i> .

				efisiensi aplikasi enterprise.	penyimpanan datanya.	
8	Rawul dkk.	2025	<i>Blockchain Technology Utilization in Improving Transparency of Regional Revenue Budget Allocation</i>	Pemanfaatan transparansi <i>blockchain</i> untuk transparansi dan auditabilitas alokasi anggaran daerah.	Implementasi difokuskan pada data transaksi finansial/anggaran, bukan pada manajemen berkas/dokumen berukuran besar (<i>unstructured data</i>).	Menfokuskan penggunaan <i>blockchain</i> khusus sebagai <i>Audit log Metadata & Integrity Checker</i> untuk file berukuran besar yang disimpan di MinIO.
9	Swastika dkk.	2022	<i>Rancang Bangun Website Akademik dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain</i>	Penerbitan dan validasi ijazah/sertifikat digital akademik agar tidak dapat dipalsukan menggunakan <i>blockchain</i> .	Penyimpanan file masih bergantung pada <i>Web server</i> konvensional (database relasional/folder biasa), <i>blockchain</i> hanya untuk transaksi sertifikat.	Mengamankan seluruh infrastruktur penyimpanan (<i>Private Storage</i>) dengan mengkombinasikan MinIO + Kontainerisasi + <i>Private Blockchain 1-Node</i> .
10	Zulkarnain & Amien	2025	<i>Optimizing MSME Product Authenticity Verification in Decentralized Markets Using Blockchain</i>	Otentikasi dan verifikasi keaslian produk UMKM pada pasar terdesentralisasi berbasis	Penerapan terfokus pada rantai pasok (<i>supply chain</i>) produk fisik, bukan pada infrastruktur penyimpanan data internal lembaga/instansi.	Mengadaptasi teknologi keaslian <i>blockchain</i> untuk membangun <i>Private Cloud Storage</i> enterprise yang memiliki jejak

				<i>blockchain.</i>		audit <i>immutable.</i>
--	--	--	--	--------------------	--	----------------------------

2.2. Landasan Teori

2.2.1 Konsep Cloud Storage dan Keamanan Berkas

Private Cloud Storage merupakan arsitektur penyimpanan data terisolasi di mana seluruh infrastruktur pemrosesan, media penyimpanan fisik, dan kontrol jaringan dikelola secara khusus untuk satu organisasi (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024). Berbeda dari penyedia layanan awan publik (*public cloud*) yang membagi sumber daya antarpengguna (*multi-tenancy*), *Private cloud* memberikan wewenang penuh kepada pihak internal untuk mengendalikan kebijakan keamanan data secara independen.

Penerapan *Private cloud storage* di SMK XYZ ditujukan untuk memberikan fleksibilitas akses dokumen akademik tanpa mengorbankan privasi data. Dalam merancang sistem pengarsipan ini, kerangka kerja keamanan informasi disandarkan pada tiga prinsip utama *CIA Triad*:

- a. *Confidentiality* (Kerahasiaan): Memastikan arsip ijazah alumni dan salinan laporan PKL hanya dapat diakses oleh pihak yang sah. Perlindungan ini diterapkan melalui mekanisme autentikasi *JSON Web Token* (JWT) dan pembatasan wewenang berdasar peran (*Role-Based Access Control* / RBAC) (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024).
- b. *Integrity* (Integritas): Menjamin bahwa setiap berkas ijazah dan nilai laporan PKL tidak mengalami perubahan, kerusakan, atau pemalsuan tanpa izin. Prinsip ini dijaga menggunakan perhitungan fungsi *hash* SHA-256 serta pembentukan rantai data *blockchain* (Abidin & Munggaran, 2025; Swastika dkk., 2022).
- c. *Availability* (Ketersediaan): Memastikan platform verifikasi arsip dapat diakses oleh staf sekolah, alumni, maupun instansi penilai secara stabil kapan saja.

Ketersediaan ini ditunjang oleh penggunaan jalur *Cloudflare Tunnel* tanpa perlu bergantung pada aplikasi VPN lokal (Hidra Amnur & Putri, 2025).

2.2.2 Object Storage MinIO dan Virtualisasi Server

MinIO merupakan perangkat lunak *object storage open-source* berkinerja tinggi yang mendukung penuh protokol S3 API (Oktaviani & Pramudyo, 2024). Tidak seperti sistem berkas tradisional yang mengorganisasi data dalam hierarki folder bertingkat, MinIO mengelola data sebagai objek mandiri di dalam sebuah wadah (*bucket*). Setiap objek di dalam MinIO tersusun atas tiga komponen mendasar:

- a. Payload Data: Berkas biner asli dokumen ijazah atau laporan PKL siswa berformat PDF (Kang dkk., 2022).
- b. System Metadata: Informasi teknis otomatis yang mencakup ukuran berkas, waktu pengunggahan, jenis MIME, dan identitas data (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024).
- c. User-Defined Metadata: Label kontekstual tambahan yang disematkan sistem, seperti NISN, Nama Alumni, ID Pengunggah, serta nilai *hash* awal berkas (Abidin & Munggaran, 2025).

Untuk menjaga integritas data fisik, MinIO dijalankan di atas lingkungan Virtual berbasis Ubuntu Server 22.04 LTS yang disimulasikan menggunakan *hypervisor VMware Workstation Pro*. Penggunaan *volume mounting* menghubungkan direktori penyimpanan MinIO secara langsung ke partisi Hard Disk Drive (HDD) fisik khusus pada jalur `/mnt/cloud-storage`. Metode ini memastikan berkas fisik tetap tersimpan aman di harddisk lokal meskipun kontainer *Docker* atau Virtual *machine* mengalami penghentian mendadak.

2.2.3 Private Blockchain dan Konsensus Internal

Private Blockchain merupakan buku besar terdistribusi (*distributed ledger*) yang membatasi hak akses pencatatan dan partisipasi jaringan hanya pada *Node-Node* terverifikasi (Kang dkk., 2022; Rawul dkk., 2025). Berbeda dari *public blockchain* yang

membutuhkan sumber daya komputasi tinggi untuk proses konsensus *Proof-of-Work* (PoW) serta membebankan biaya transaksi (*gas fee*), *Private blockchain* menawarkan pemrosesan log yang instan dan tanpa biaya (Abidin & Munggaran, 2025).

Node Private blockchain pada sistem ini dikemas ke dalam satu unit kontainer *Docker*. *Node* tersebut menjalankan *Smart Contract* yang bertugas mencatat setiap jejak aktivitas (*audit log*) saat dokumen ijazah atau laporan PKL diunggah, diperbarui, atau dihapus. Blok yang tercipta mengunci informasi penting yang meliputi urutan blok (*index*), penanda waktu (*timestamp*), *hash* berkas fisik, *hash* metadata, *hash* blok sebelumnya (*previous hash*), dan *hash* blok saat ini (*current hash*) (Swastika dkk., 2022).

2.2.4 Algoritma SHA-256 dan Skema *Hash-Chaining*

SHA-256 (*Secure Hash Algorithm 256-bit*) adalah fungsi *hash kriptografi* searah yang memetakan masukan data biner berukuran berapa pun menjadi deretan karakter acak sepanjang tetap 256 bit (Abidin & Munggaran, 2025). Algoritma ini dirancang *one-way*, sehingga secara matematis tidak mungkin mengembalikan nilai *hash* menjadi isi berkas semula (Noman & Gwenhure, 2025).

Sistem menerapkan skema rantai *hash* (*hash-chaining*) untuk menjamin *immutability* (Oktaviani & Pramudyo, 2024). Blok pencatatan baru (N) disusun dengan menyertakan nilai *hash* dari blok sebelumnya ($N - 1$). Formulasi perhitungan *hash* blok ke- N dirumuskan sebagai berikut:

$$H_N = \text{SHA-256}(\text{Index}_N \parallel \text{Timestamp}_N \parallel \text{HashFile}_N \parallel \text{Actor}_N \parallel H_{N-1})$$

Operasi $\parallel$ menunjukkan penggabungan string (*concatenation*). Karakteristik *Avalanche Effect* pada SHA-256 memastikan bahwa perubahan sekecil satu bit saja pada isi berkas PDF ijazah/PKL fisik di MinIO akan menghasilkan nilai *hash* yang sama sekali berbeda (Abidin & Munggaran, 2025). Ketidakcocokan nilai ini otomatis memutus keterikatan rantai blok dan menandai berkas telah mengalami pemalsuan atau manipulasi (*tampering*) (Swastika dkk., 2022).

Tabel 2. 2 Algoritma SHA-256

Variabel	Komponen Data	Keterangan
H_N	<i>Current Hash</i>	Nilai <i>hash</i> enkripsi SHA-256 yang dihasilkan untuk blok ke- N .
$Index_N$	<i>Block Index</i>	Urutan nomor indeks dari blok data transaksi/log.
$Timestamp_N$	<i>Time Stamping</i>	Catatan waktu (tanggal, jam, detik) saat transaksi dibuat.
$HashFile_N$	<i>File Hash</i>	Nilai <i>hash</i> SHA-256 dari berkas fisik (PDF ijazah/laporan PKL).
$Actor_N$	<i>User Identity</i>	Identitas/ID pengguna yang melakukan aksi atau pengunggahan data.
H_{N-1}	<i>Previous Hash</i>	Nilai <i>hash</i> dari blok sebelumnya ($N - 1$) yang membentuk rantai (<i>chain</i>).
$\parallel$	<i>Concatenation</i>	Simbol penggabungan (<i>string concatenation</i>) antar variabel input.

2.2.5 Kontainerisasi *Docker* dan Arsitektur *Microservices*

Docker merupakan teknologi Virtualisasi berbasis tingkat sistem operasi (*OS-level Virtualization*) yang mengisolasi aplikasi ke dalam kontainer ringan (Fauzi & Suka, 2025). Tidak seperti mesin Virtual konvensional yang harus menginstal sistem operasi *guest* utuh di atas *hypervisor*, *Docker* memanfaatkan kernel dari OS *host* secara langsung, sehingga sangat menghemat penggunaan memori RAM dan CPU.

Pendekatan *Microservices* mengisolasikan modul aplikasi ke dalam komponen independen. Komponen *storage* (MinIO), *backend gateway* (Flask API), basis data (MySQL), dan *blockchain Node* masing-masing berjalan di kontainer tersendiri serta saling berkomunikasi melalui jaringan internal *Docker* (*bridge network*). Jika salah satu layanan mengalami gangguan, modul lain tetap dapat beroperasi tanpa memicu keruntuhan sistem secara keseluruhan (*fault tolerance*) (Hidra Amnur & Putri, 2025).

2.2.6 Otentikasi JSON Web Token (JWT) dan Role-Based Access Control (RBAC)

Otentikasi bertindak sebagai pintu utama untuk menguji identitas pengguna sebelum memberikan hak akses. Sistem ini menerapkan standar *JSON Web Token* (JWT) yang bersifat *stateless*, sehingga server tidak perlu menyimpan informasi sesi pengguna di dalam memori. Struktur token JWT terdiri dari *Header* (informasi algoritma), *Payload* (data identitas & peran), dan *Signature* (kunci pemasti otentisitas).

Untuk mengontrol wewenang pada sistem pengarsipan SMK XYZ, diterapkan *Role-Based Access Control* (RBAC) dengan pembagian 3 aktor utama (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024):

- a. Administrator (Staf Tata Usaha / TU): Memegang wewenang penuh dalam mengelola data alumni, mengunggah dan mengarsipkan ijazah, menghapus berkas, mengelola akun pengguna, serta memantau *audit log*.
- b. Pengguna (Guru Pembimbing PKL): Memiliki hak untuk mengunggah berkas laporan PKL siswa bimbingannya, mengunduh berkas laporan yang relevan, serta melihat riwayat aktivitas mandiri.
- c. Auditor (Kepala Sekolah / Waka Kurikulum / Pihak Eksternal): Memiliki hak akses khusus untuk memantau seluruh riwayat *audit log*, mengeksekusi pengujian verifikasi keaslian dokumen (*tamper detection*), serta memastikan keutuhan berkas tanpa wewenang mengubah data.

2.2.7 Aksesibilitas Terenkripsi Menggunakan Cloudflare Tunnel (Zero Trust)

Akses remote dari luar jaringan lokal sekolah dikelola mengadopsi prinsip Zero Trust Network Access (ZTNA) menggunakan layanan *Cloudflare Tunnel* (cloudflared). Metode ini meniadakan kebutuhan konfigurasi port forwarding pada router sekolah serta tidak memerlukan IP publik statis.

Daemon cloudflared yang berjalan di dalam kontainer server membentuk jalur koneksi keluar (outbound) terenkripsi menuju edge server Cloudflare. Seluruh permintaan verifikasi ijazah dari luar sekolah dienkripsi menggunakan protokol SSL/TLS 1.3 dan disaring oleh *Web Application Firewall* (WAF) sebelum masuk ke

jaringan lokal. Hal ini melindungi server internal sekolah dari potensi serangan siber dari internet terbuka (Zulkarnain & Amien, 2025).

2.3. Kerangka Berfikir

Alur pemikiran yang menjadi dasar penyusunan penelitian ini dirancang secara terstruktur berdasarkan evaluasi permasalahan operasional SMK XYZ dan rujukan literatur terdahulu (Abidin & Munggaran, 2025). Visualisasi alur kerangka berpikir disajikan sebagai berikut:



Gambar 2. 1 Kerangka Berfikir

BAB III

METODE PENELITIAN

3.1. Analisis Kebutuhan

Proses analisis dilakukan untuk memastikan infrastruktur *Private cloud storage* yang dibangun sanggup mengatasi kendala pengarsipan di SMK XYZ serta memenuhi kaidah keamanan data akademik (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024). Analisis kebutuhan dikelompokkan menjadi kebutuhan fungsional dan non-fungsional.

3.1.1 Kebutuhan Fungsional (Functional Requirements)

Berikut merupakan kebutuhan non fungsional dari penelitian ini:

- a. Otentikasi Berbasis Peran (RBAC): Sistem menyediakan akses login berstandar JWT yang membagi wewenang ke dalam tiga aktor: Administrator (Staf TU), Pengguna (Guru Pembimbing), dan Auditor (Kepala Sekolah/Verifikator) (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024).
- b. Manajemen Akun Pengguna: Staf TU dapat menambah, memperbarui status, dan mencabut hak akses akun guru maupun verifikator.
- c. Penyimpanan Berkas Digital Akademik:
 - 1) Staf TU dapat mengunggah dokumen ijazah alumni (PDF) disertai metadata (NISN, Nama Alumni, Tahun Lulus) ke *bucket* MinIO (Kang dkk., 2022).
 - 2) Guru Pembimbing dapat mengunggah berkas laporan PKL siswa bimbingannya.

- d. Pengunduhan Dokumen Terproteksi: Pengunduhan berkas dibatasi oleh hak akses peran guna mencegah kebocoran dokumen rahasia (Devina Oktaviani & Gani Nur Pramudyo, S.IP., 2024).
- e. Pencatatan *Audit log* Otomatis: Setiap transaksi unggah atau hapus dokumen fisik secara otomatis memicu pembuatan nilai *hash* SHA-256 yang dikunci pada rantai *blockchain* (Abidin & Munggaran, 2025; Swastika dkk., 2022).
- f. Verifikasi Keaslian Dokumen (Tamper Detection): Sistem menyediakan antarmuka untuk membandingkan *hash* berkas fisik di MinIO dengan *hash* terdaftar di *blockchain* guna memverifikasi keaslian ijazah/PKL secara otomatis.
- g. Visualisasi *Audit log*: Sistem menyajikan tabel rekam aktivitas secara transparan bagi seluruh aktor yang memiliki hak akses (Rawul dkk., 2025).

3.1.2 Kebutuhan Non-Fungsional (Non-Functional Requirements)

Berikut merupakan kebutuhan non fungsional dari penelitian ini:

- a. Keamanan Komunikasi Data: Seluruh lalu lintas data eksternal dienkripsi menggunakan SSL/TLS 1.3 via *Cloudflare Tunnel* tanpa perlu membuka port *inbound* pada router sekolah.
- b. Efisiensi Memori Server: Konsumsi RAM gabungan untuk seluruh kontainer *Docker* (*storage-service*, *blockchain-service*, *dashboard-Web*, *MySQL*) tidak boleh melebihi 2 GB (2048 MB) pada kondisi *idle* (Sudirman & Hermawan, 2025).
- c. Keandalan Sistem: Kontainer menggunakan kebijakan *auto-restart* agar layanan langsung pulih secara mandiri apabila terjadi kemacetan (*crash*).
- d. Kecepatan Komputasi: Proses kalkulasi *hash* SHA-256 hingga pencatatan blok baru untuk berkas hingga 10 MB harus selesai di bawah 3 detik (Abidin & Munggaran, 2025).

3.2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif-eksperimental melalui pengujian langsung pada infrastruktur server yang dibangun. Pengumpulan data dilaksanakan melalui tiga teknik utama:

- a. Observasi Langsung: Mengamati proses penataan fisik ijazah di ruang Tata Usaha (TU) SMK XYZ, mengevaluasi kendala penyebaran laporan PKL pada laptop guru, serta memeriksa spesifikasi server sekolah.
- b. Studi Literatur: Menganalisis 10 artikel jurnal bereputasi terkait *Private cloud storage*, kontainerisasi *Docker*, algoritma *SHA-256*, *Private blockchain*, dan *Cloudflare Tunnel*.
- c. Eksperimentasi Laboratorium: Melakukan pengujian fungsionalitas (*Black-box Testing*) dan pengujian manipulasi (*Tamper Detection Testing*) pada lingkungan server lokal berbasis *VMware*. Pengujian berfokus pada evaluasi konsumsi sumber daya (CPU, RAM, Disk I/O) serta ketahanan sistem dalam mendeteksi perubahan isi berkas ijazah/PKL (Swastika dkk., 2022).

3.3. Metode Pengembangan Sistem

3.3.1 Kerangka Penelitian (NDLC)

Penelitian dilaksanakan mengikuti tahapan *Network Development Life Cycle* (NDLC):

- a. *Analysis*: Identifikasi permasalahan pengarsipan di SMK XYZ, analisis kebutuhan 3 aktor (TU, Guru, Auditor), dan tinjauan literatur.
- b. *Design*: Merancang topologi jaringan, arsitektur *Microservices*, diagram DFD/UML, skema basis data MySQL (tabel *users*, *folders*, *files*, *file_versions*, *file_permissions*, *audit_logs*, *integrity_records*), serta *wireframe UI*.
- c. *Simulation Prototyping*: Instalasi OS Ubuntu Server di *VMware*, penautan partisi HDD fisik ke `/mnt/cloud-storage`, serta penyusunan skrip *Docker-compose.yml*.

- d. *Implementation*: Penulisan skrip Flask API (*blockchain-service*), modul otentikasi JWT, integrasi MinIO S3 API, serta penyambungan *Cloudflare Tunnel*.
- e. *Testing*: Pengujian pengunggahan ijazah/PKL (PDF), validasi RBAC 3 aktor, pengujian verifikasi remote, dan simulasi pengeditan paksa berkas fisik.
- f. *Management*: Penyusunan dokumentasi teknik, SOP operasional pengarsipan sekolah, konfigurasi *auto-restart*, dan penyelesaian draf skripsi.

3.3.2 Arsitektur dan Spesifikasi Teknis

Sistem mengintegrasikan spesifikasi perangkat keras dan lunak berikut:

- a. *Host Hardware*: PC Server *dedicated* (Windows OS, CPU Intel/AMD dengan Virtualization Enabled, RAM 8-16 GB, HDD Dedicated Storage).
- b. *Virtualization Layer*: *VMware Workstation Pro* menjalankan Ubuntu Server 22.04 LTS (Network Adapter: Bridged).
- c. *Storage Partition*: *Harddisk* fisik kedua di-mount ke jalur */mnt/cloud-storage* khusus untuk *volume* MinIO.
- d. *Docker Compose Services*:
 - 1) *storage-service* (MinIO): *Port* 9000/9001 internal sebagai *Object Storage*.
 - 2) *blockchain-service* (*Flask API & MySQL DB*): *Port* 5000 untuk kelola JWT, MinIO, dan pembentukan rantai *hash-chain*.
 - 3) *dashboard-Web* (Nginx): *Port* 8080 untuk menyajikan 3 antarmuka *custom dashboard*.
- e. *Network Gateway*: *Cloudflare Tunnel* (*cloudflared*) untuk mempublikasikan layanan via HTTPS tanpa *port forwarding*.

3.4. Jadwal Penelitian

Berikut merupakan jadwal penelitian yang menggambarkan tahapan kegiatan beserta alokasi waktu pelaksanaannya:

Tabel 3. 1 Jadwal Penelitian

No	Nama Kegiatan	Jadwal Pelaksanaan (2026–2027)					
		Agu–Sep '26	Okt–Nov '26	Des '26– Jan '27	Feb–Mar '27	Apr–Mei '27	Jun–Jul '27
1	Penyusunan Draft Proposal Skripsi (Bab 1– 3)						
2	Pendaftaran & Sidang Pra-UAPS (Sempro)						
3	Observasi Lapangan & Analisis Kebutuhan Sistem SMK XYZ						
4	Perancangan Sistem (Arsitektur, Database & UI/UX)						
5	Persiapan <i>Environment</i> Server (<i>VMware</i> & <i>Docker</i>)						

6	Implementasi Sistem (MinIO, <i>Flask API</i> , JWT & <i>Blockchain</i>)						
7	Pengujian Sistem (<i>Black-Box Testing</i> & Integrasi RBAC)						
8	Evaluasi Performa Server & Deteksi Manipulasi Berkas						
9	Penyusunan Laporan Akhir Skripsi & Persiapan Sidang Skripsi						

DAFTAR PUSTAKA

- Abidin, M. F., & Munggaran, L. C. (2025). Blockchain-Based Digital Document Verification Using SHA-256 on the Internet Computer Protocol (ICP). *Journal of Electrical, Electronic, Information, and Communication Technology*, 7(2), 64. <https://doi.org/10.20961/jeeict.7.2.108624>
- Almotawkel, N. A. A., & Obaid, A. M. H. (2026). Balancing Secrecy and Transparency in Smart Cities: a Systematic Review of Blockchain-Based Government Data Management. *Jurnal Pilar Nusa Mandiri*, 22(1), 50–68. <https://doi.org/10.33480/pilar.v22i1.8254>
- Devina Oktaviani, & Gani Nur Pramudyo, S.IP., M. H. (2024). Literature Review: Preservasi Penyimpanan Arsip Elektronik dalam Keamanan Arsip Mengguakan Teknologi Blockchain. *Sabda*, Volume 17, 25–41. <https://doi.org/10.14710/sabda.17.2.25-41>
- Hidra Amnur, & Putri, W. A. (2025). Zerotier Pada Home Server Menggunakan Sistem Operasi CasaOS. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, 6(2), 163–169. <https://doi.org/10.62527/jitsi.6.2.467>
- Kang, P., Yang, W., & Zheng, J. (2022). Blockchain Private File Storage-Sharing Method Based on IPFS. *Sensors*, 22(14), 1–12. <https://doi.org/10.3390/s22145100>
- Noman, E. P., & Gwenthure, A. K. (2025). Factors Influencing the Diffusion of Blockchain Technology in the Indonesian Goverment. *Journal of Information Systems Engineering and Business Intelligence*, 11(2), 215–225. <https://doi.org/10.20473/jisebi.11.2.215-225>
- Rahmatulloh, A., Gunawan, R., & Rizal, R. (2025). Arsitektur Microservice untuk Optimalisasi Aplikasi Eco-Maps dalam Mendukung Kampus Ramah Lingkungan. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 10(3), 341–350.

<https://doi.org/10.14421/jiska.2025.10.3.341-350>

- Rawul, W. A., Zahwa, M. F., Roshan, R., & Mawar. (2025). Blockchain Technology Utilization in Improving Transparency of Regional Revenue Budget Allocation. *Spirit Publik: Jurnal Administrasi Publik*, 20(1), 167–186.
- Swastika, W., Wirasantosa, H., & Kelana, O. H. (2022). Rancang Bangun Website Akademik dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 9(1), 33. <https://doi.org/10.25126/jtiik.2021863645>
- Zulkarnain, A., & Amien, M. (2025). Optimizing Msme Product Authenticity Verification in Decentralized Markets Using Blockchain. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, 10(3), 554–564. <https://doi.org/10.33480/jitk.v10i3.6010>