PENERAPAN METODE PROTOTYPING PADA PERANCANGAN *PRIVATE CLOUD STORAGE* BERBASIS TELEGRAM BOT MELALUI PROTOKOL MTPROTO DENGAN ALGORITMA KRIPTOGRAFI AES-256

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika Fakultas Teknik dan Pertanian Universitas Islam Nusantara Bandung

Disusun Oleh:

FAISHAL MUHAMMAD NAUFA

41037006221004

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN PERTANIAN

UNIVERSITAS ISLAM NUSANTARA

BANDUNG

2026

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

Judul Proposal	:	Penerapan Metode Prototyping Pada Perancangan Private Cloud Storage Berbasis Telegram Bot Melalui Protokol Mtproto Dengan Algoritma Kriptografi AES-256
Nama	:	Faishal Muhammad Naufa
NIM	:	41037006221004
Program Studi	:	Teknik Informatika

Tanggal Lulus: 28 Juli 2026

Disetujui oleh,

Pembimbing I,	Pembimbing II,
Muhamad Ikmal Wiawan, M.Kom	Galih, S.T., M.Kom.
NIDN. 0429089401	NIDN. 0427068707

Diketahui oleh,

Dekan,	Ketua Program Studi,
Dr. Bobby Ustari, S.P., M.P.	Dr. Ir. Tedjo Darmanto, S.T., M.T.
NIDN. 0401129202	NIDN. 8959250022

FTP UNIMUS
Fakultas Teknik dan Perencana

HALAMAN PENGESAHAN SIDANG

HALAMAN PENGESAHAN SIDANG

Judul Proposal	:	Penerapan Metode Prototyping Pada Perancangan Private Cloud Storage Berbasis Telegram Bot Melalui Protokol Mtproto Dengan Algoritma Kriptografi AES-256
Nama	:	Faishal Muhammad Naufa
NIM	:	41037006221004
Program Studi	:	Teknik Informatika

Telah dipertahankan di depan dewan penguji dalam sidang tugas akhir:

Hari : Selasa
Tanggal : 28 Juli 2026

Disetujui,

Ketua Sidang	:	Siti Nur, S.ST., M.Kom. NIDN. 0425058705	.....
Penguji 1	:	Dr. Ir. Tedjo Darmanto, S.T., M.T. NIDN. 8959250022	.....
Penguji 2	:	Yenni Fatman, S.T., M.T. NIDN. 0403048106	.....

LEMBAR PERNYATAAN

Yang bertandatangan di bawah ini:

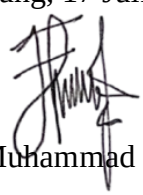
Nama	:	Faishal Muhammad Naufa
NIM	:	41037006221004
Fakultas	:	Teknik dan Pertanian
Program Studi	:	Teknik Informatika
Judul Tugas Akhir	:	Penerapan Metode Prototyping Pada Perancangan Private Cloud Storage Berbasis Telegram Bot Melalui Protokol MTProto Dengan Algoritma Kriptografi AES-256.

Dengan ini menyatakan:

1. Tugas Akhir ini merupakan hasil karya saya sendiri, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat orang lain yang ditulis atau di terbitkat sebelumnya, kecuali yang secara tertulis dikutip dan diacu dalam naskah ini sesuai kode etik ilmiah
2. Data informasi, dan hasil analisis yang di sajikan adalah valid, terukur, dan dapat, dipertanggung jawabkan secara akademik, serta tidak mengandung unsur manipulasi atau fabrikasi data.
3. Apabila di kemudian hari terbukti terdapat plagiarisme, pemalsuan data, atau pelanggaran integritas akademik lainya, saya bersedia menerima sanksi akademik sesuai peraturan yang berlaku di Universitas Islam Nusantara, termasuk pembatalan gelar yang telah diperoleh.

Demikian pernyataan ini saya buat dengan sebenar-benarnya, tanpa ada pemaksaan dari pihak mana pun, untuk dipergunakan sebagaimana mestinya.

Bandung, 17 Juli 2026



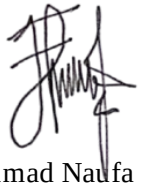
Faishal Muhammad Naufa

41037006221004

LEMBAR PERSEMBAHAN

Puji dan syukur senantiasa penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala limpahan rahmat serta karunia-Nya, sehingga penyusunan Tugas Akhir yang berjudul "**PENERAPAN METODE PROTOTYPING PADA PERANCANGAN PRIVATE CLOUD STORAGE BERBASIS TELEGRAM BOT MELALUI PROTOKOL MTPROTO DENGAN ALGORITMA KRIPTOGRAFI AES-256**" dapat diselesaikan dengan baik. Karya tulis ini disusun guna memenuhi salah satu syarat akademis dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Fakultas Teknik dan Pertanian, Universitas Islam Nusantara. Penulisan Tugas Akhir ini ditujukan untuk memaparkan proses perancangan dan pengembangan sistem *Private Cloud Storage* berbiaya rendah yang memanfaatkan infrastruktur server Telegram. Penulis menaruh harapan besar agar sistem yang mengintegrasikan protokol MTProto dan enkripsi data tingkat tinggi ini mampu menjadi solusi penyimpanan berkas berskala besar yang efisien, aman, serta terjamin privasinya tanpa memerlukan *hosting* server tambahan.

Bandung, 17 Juli 2026



Faishal Muhammad Naufa NIM
41037006221004

PENERAPAN METODE PROTOTYPING PADA PERANCANGAN *PRIVATE CLOUD STORAGE* BERBASIS TELEGRAM BOT MELALUI PROTOKOL MTPROTO DENGAN ALGORITMA KRIPTOGRAFI AES-256

Faishal Muhammad Naufa
Program Studi Teknik Informatika, Fakultas Teknik
Universitas Islam Nusantara

ABSTRAK

Meningkatnya kebutuhan penyimpanan data digital dihadapkan pada keterbatasan kapasitas gratis dan tingginya biaya layanan *cloud storage* komersial. Membangun infrastruktur *server* fisik secara mandiri juga membutuhkan biaya pemeliharaan yang besar. Penelitian ini bertujuan untuk mengatasi masalah tersebut dengan merancang sistem *Private Cloud storage* berbiaya rendah yang memanfaatkan infrastruktur *server* Telegram. Sistem dibangun menggunakan metode *Prototyping* dengan mengintegrasikan antarmuka *Web UI*, pustaka Pyrogram untuk komunikasi langsung ke *data center* Telegram melalui protokol biner *MTProto*, serta basis data SQLite. Untuk menjamin keamanan dan privasi, data dienkripsi secara lokal di sisi *backend* menggunakan algoritma AES-256-CBC, sedangkan integritasnya diverifikasi menggunakan fungsi *hash SHA-256*. Selain itu, batasan kapasitas transfer *native* Telegram diatasi melalui implementasi teknik *file chunking* otomatis untuk memecah berkas yang berukuran lebih dari 1,8 GB. Hasil pengujian menunjukkan bahwa sistem berhasil mengunggah, mengenkripsi, memecah, dan merekonstruksi kembali berkas tanpa kegagalan atau kerusakan data. Kesimpulannya, penggabungan protokol MTProto dan teknik *file chunking* terbukti efektif menghadirkan solusi penyimpanan awan berskala besar, efisien, dan aman tanpa memerlukan *hosting server* perantara tambahan.

Kata Kunci: *Private Cloud storage, Telegram Bot, Protokol MTProto, AES-256, File chunking, Prototyping.*

PENERAPAN METODE PROTOTYPING PADA PERANCANGAN *PRIVATE CLOUD STORAGE* BERBASIS TELEGRAM BOT MELALUI PROTOKOL MTPROTO DENGAN ALGORITMA KRIPTOGRAFI AES-256

Faishal Muhammad Naufa
Program Studi Teknik Informatika, Fakultas Teknik
Universitas Islam Nusantara

ABSTRACT

The increasing need for digital data storage faces challenges due to the limited free capacity and high costs of commercial cloud storage services. Building independent physical server infrastructure also requires massive maintenance costs. This research aims to address these problems by designing a low-cost Private Cloud storage system that utilizes Telegram's server infrastructure. The system was developed using the Prototyping method by integrating a Web UI, the Pyrogram library for direct communication to Telegram data centers via the MTProto binary protocol, and an SQLite database. To ensure security and privacy, data is locally encrypted on the backend using the AES-256-CBC algorithm, while its integrity is verified using the SHA-256 hash function. Furthermore, the native Telegram transfer limit was bypassed by implementing an automatic file chunking technique to split files larger than 1.8 GB. Testing results indicate that the system successfully uploads, encrypts, splits, and reassembles files without data failure or corruption. In conclusion, combining the MTProto protocol and file chunking techniques is proven effective in providing a large-scale, efficient, and secure cloud storage solution without requiring additional intermediary server hosting.

Keywords: *Private Cloud storage, Telegram Bot, MTProto Protocol, AES-256, File chunking, Prototyping.*

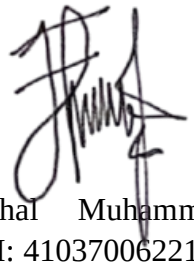
KATA PENGANTAR

Segala puji dan syukur senantiasa penulis panjatkan ke hadirat Allah SWT, karena berkat limpahan rahmat serta karunia-Nya, penyusunan tugas akhir ini dapat diselesaikan dengan baik. Melalui kesempatan ini, penulis ingin menghaturkan ucapan terima kasih yang tulus kepada seluruh pihak yang telah memberikan dukungan dan bantuan. Dengan penuh rasa syukur, tugas akhir ini penulis persembahkan untuk:

1. **Prof. Dr. Endang Komara, M.Si.,** selaku Rektor Universitas Islam Nusantara, atas segala arahan, kebijakan, dan fasilitas akademik yang sangat mendukung kelancaran proses perkuliahan dan penyusunan Tugas Akhir penulis.
2. **Bapak Dr. Tedjo Darmanto, S.T., M.T.**, selaku Ketua Program Studi Teknik Informatika Universitas Islam Nusantara, atas kesempatan, fasilitas, dan dukungan yang diberikan selama penulis menempuh pendidikan.
3. Bapak **Muhamad Ikmal Wiawan, S.Tr. Kom., M.Kom.,** selaku Dosen Pembimbing I, yang telah dengan penuh kesabaran meluangkan waktu, tenaga, dan pikirannya untuk memberikan bimbingan, arahan, serta ilmu yang sangat berharga di tengah kesibukan beliau.
4. Bapak **Galih, S.T., M.Kom.**, selaku Dosen Pembimbing II, yang tak lelah memberikan dukungan moral, masukan kritis, dan solusi atas berbagai kendala yang penulis hadapi selama merancang dan menyusun Tugas Akhir ini.
5. **Kedua Orang Tua tercinta**, atas doa yang tak pernah putus, pengorbanan yang tak terhingga, serta kasih sayang luar biasa yang selalu menjadi penguat dan alasan utama penulis untuk tidak pernah menyerah hingga berada di titik ini.
6. **Kepada teman-teman seperjuangan**, yang selalu hadir untuk saling mendukung, menemani proses diskusi, dan memberikan semangat di saat-saat penulis merasa kesulitan dalam menyelesaikan Tugas Akhir ini.
7. **Kepada seseorang dari Universitas Jambi** yang menjadi bagian penting dalam perjalanan ini, terima kasih atas segala bentuk dukungan, motivasi, dan pelajaran berharga yang telah diberikan hingga penulis dapat menyelesaikan Tugas Akhir ini.

Semoga Allah SWT senantiasa memberikan perlindungan, rahmat, serta karunia-Nya kepada semua pihak yang telah banyak membantu. Penulis berharap segala keikhlasan dalam berbagi ilmu serta dukungan moril dan materi yang telah diberikan, dapat menjadi amal jariah yang pahalanya terus mengalir. Aamiin ya Rabbal 'aalamiin.

Bandung, 17 Juli 2026



Faishal Muhammad Naufa
NIM: 41037006221004

DAFTAR ISI

HALAMAN PENGESAHAN ..... **ii**

HALAMAN PENGESAHAN SIDANG ..... **ii**

LEMBAR PERNYATAAN ..... **iv**

LEMBAR PERSEMBAHAN ..... **v**

ABSTRAK ..... **vi**

ABSTRACT ..... **vii**

KATA PENGANTAR ..... **viii**

DAFTAR ISI ..... **x**

DAFTAR GAMBAR ..... **xiv**

DAFTAR TABEL ..... **xvi**

DAFTAR ISTILAH DAN SINGKATAN ..... **xvii**

BAB I PENDAHULUAN **1**

1.1. Latar Belakang 1

1.2. Rumusan Masalah 3

1.3. Tujuan Penelitian 4

1.4. Batasan Masalah 4

1.5 Manfaat Penelitian 5

1.5.1. Manfaat Teoritis 5

1.5.2. Manfaat Praktis 6

1.6. Jadwal Penelitian 7

1.7 Sistematika Penulisan 8

BAB II TINJAUAN PUSTAKA **9**

2.1 *State of The Art* 9

2.2 Penelitian Terdahulu 14

2.3 Kajian Teori 16

2.3.1 *Private Cloud storage* dan *Virtual file manager* 16

2.3.2. Telegram Bot API dan Protokol MTProto 17
2.3.3. Teknik *File chunking* 19
2.3.4. Kriptografi dan Algoritma AES-256 21
2.3.5. Metode Prototyping 22
2.3.6 Python 24
2.3.7 Flask 24
2.3.8. Gunicorn dan WSGI 25
2.3.9 SQLite 26
2.3.10 JSON Web *Token* 26
2.3.11 Bcrypt 27
2.3.12 PBKDF2 (*Password-Based Key Derivation Function 2*) 27
2.3.13 *Black-Box* Testing 28
2.4. UML (*Unified Modeling Language*) 28
2.4.1 *Use case Diagram* 28
2.4.2 *Class Diagram* 29
2.4.3 *Activity Diagram* 30
2.4.4 *Sequence Diagram* 31
2.4.5 *Entity Relationship Diagram* (ERD) 32
BAB III METODOLOGI PENELITIAN 32
3.1. Metode Penelitian 32
3.2. Lokasi dan Waktu Penelitian 32
3.3. Objek dan Subjek Penelitian 33
3.3.1. Objek Penelitian 33
3.3.2. Subjek Penelitian 34
3.4. Alat dan Bahan Penelitian 34
3.5. Teknik Pengumpulan Data 35
3.6. Prosedur Penelitian 36

3.6.1. Identifikasi Masalah 39
3.6.2. Studi Literatur 39
3.6.3. Analisis Sistem yang Berjalan 39
3.6.4. Analisis Kebutuhan Sistem 41
3.6.5. Perancangan *Prototype* 42
3.6.6. Implementasi Sistem 60
3.6.7. Implementasi Enkripsi 61
3.6.8. Implementasi *File chunking* 61
3.6.9. Pengujian Sistem 61
3.6.10. Evaluasi *Prototype* 62
3.6.11. Penyempurnaan Sistem 62
3.6.12. Penyusunan Laporan Akhir 62
3.7. Pengolahan dan Analisis Data 62
BAB IV HASIL DAN PEMBAHASAN 63
4.1. Hasil Implementasi Sistem 63
4.1.1. Implementasi Antarmuka Pengguna (*Web UI*) 63
4.1.2. Implementasi *Database* dan *Backend* 67
4.1.3. Implementasi Lingkungan Produksi (*Production Deployment*) 68
4.2. Hasil Implementasi Keamanan dan Kriptografi 69
4.2.1. Implementasi Autentikasi JWT dan Bcrypt 69
4.2.2. Implementasi Enkripsi AES-256-CBC 71
4.2.3. Implementasi *File chunking* 73
4.3. Pengujian Sistem 75
4.3.1. Pengujian Fungsional (*Black-Box* Testing) 75
4.3.2. Pengujian Kriptografi dan Integritas (SHA-256) 82
4.3.3. Pengujian Performa 84
4.4 Evaluasi *Prototype* 87

4.5 Pengujian *Usability* (*User Acceptance Test*)..... 88
4.6 Kelebihan dan Keterbatasan Sistem..... 91
4.6.1 Kelebihan Sistem 91
4.6.2 Keterbatasan Sistem..... 92
BAB V KESIMPULAN DAN SARAN 90
5.1. Kesimpulan 90
5.2. Saran..... 91
DAFTAR PUSTAKA 93
LAMPIRAN..... 96
Lampiran 1 Dokumentasi Pengujain Sistem..... 96
Lampiran 2 Hasil Data Kuisoner..... 97
Lampiran 3 Pengujian *Production* Oleh Dosen Pembimbing..... 97
Lampiran 4 Repository Github..... 98
Lampiran 5 Informasi Spesifikasi VPS 98
Lampiran 6 Lampiran Surat Keterangan Bebas Plagiasi 99
RIWAYAT HIDUP PENULIS..... 100

DAFTAR GAMBAR

Gambar 2. 1 Metode Prototyping 23
Gambar 2. 2 Arsitektur Komunikasi WSGI Server dan Web Server 26
Gambar 2. 3 Contoh ERD 33
Gambar 3. 1 Flowchart Tahapan Penelitian dengan Metode Prototyping 37
Gambar 3. 2 Alur Sistem Eksisting Pengunggahan Berkas secara Manual 40
Gambar 3. 3 Use case Diagram Sistem Private Cloud storage 43
Gambar 3. 4 Activity Diagram Autentikasi 47
Gambar 3. 5 Activity Diagram Upload File 49
Gambar 3. 6 Activity Diagram Download File 51
Gambar 3. 7 Sequence Diagram Autentikasi (Login) 52
Gambar 3. 8 Sequence Diagram Upload File 52
Gambar 3. 9 Sequence Diagram Download File 53
Gambar 3. 10 Class Diagram 53
Gambar 3. 11 Entity Relationship Diagram (ERD) Basis Data Metadata 55
Gambar 3. 12 Arsitektur Keseluruhan Sistem Private Cloud storage 57
Gambar 3. 13 Deployment Diagram Private Cloud storage 58
Gambar 3. 14 Wireframe Halaman Autentikasi Login 59
Gambar 3. 15 Wireframe Halaman Autentikasi Registrasi 59
Gambar 3. 16 Wireframe Halaman Dashboard Utama 60
Gambar 4. 1 Tampilan Halaman Registrasi Sistem 64
Gambar 4. 2 Tampilan Halaman Registrasi Sistem pada kredensial Telegram 64
Gambar 4. 3 Tampilan Halaman Login Sistem 65
Gambar 4. 4 Tampilan Dashboard Utama 65
Gambar 4. 5 Tampilan Dialog Unggah Berkas dengan Indikator Kemajuan 66
Gambar 4. 6 Tampilan Fitur Pencarian Berkas 66
Gambar 4. 7 Diagram Skema Basis Data SQLite 67
Gambar 4. 8 Berkas Terenkripsi yang Tersimpan di Infrastruktur Telegram 69
Gambar 4. 9 Contoh *Hash* Bcrypt yang Tersimpan di Basis Data 70
Gambar 4. 10 Penyimpanan Secret_key & Basis Data 71
Gambar 4. 11 Diagram Alur Proses Enkripsi Berkas 72
Gambar 4. 12 Perbandingan Konten Berkas Asli dan Ciphertext Terenkripsi 73
Gambar 4. 13 *Chunk* Berkas yang Diunggah Secara Sekuensial ke Telegram 75
Gambar 4. 14 Bukti Berkas Terenkripsi Tidak Dapat Dibuka Tanpa Kunci 84

Gambar 4. 15 Bukti Mekanisme File Chunking pada Berkas 2,5 GB 86
Gambar 4. 16 Hasil Evaluasi Prototype oleh Pengguna..... 91

DAFTAR TABEL

Tabel 1. 1 Jadwal Kegiatan Penelitian. 7
Tabel 2. 1 Perbandingan Penelitian Sebelumnya 9
Tabel 2. 2 Pengertian Use case Diagram 29
Tabel 2. 3 Pengertian Class Diagram 30
Tabel 2. 4 Pengertian Activity Diagram 31
Tabel 2. 5 Pengertian Sequence Diagram 32
Tabel 2. 6 Notasi ERD 34
Tabel 3. 1 Perangkat Keras Klien & Pengembangan 35
Tabel 3. 2 Perangkat Keras Server (*Virtual Private Server*) 35
Tabel 3. 3 Perangkat Lunak 35
Tabel 3. 4 Pengertian Actor Usecase 44
Tabel 3. 5 Pengertian Actor Activity Diagram 46
Tabel 3. 6 Pengertian Actor Activity Diagram Upload File 48
Tabel 3. 7 Activity Diagram Download File 50
Tabel 3. 8 Metode Pengolahan dan Analisis Data 63
Tabel 4. 1 Hasil Pengujian Fungsional Skenario Autentikasi 76
Tabel 4. 2 Hasil Pengujian Fungsional Skenario Manajemen Berkas 79
Tabel 4. 3 Hasil Pengujian Fungsional Skenario Manajemen Folder 81
Tabel 4. 4 Hasil Verifikasi Integritas SHA-256 83
Tabel 4. 5 Hasil Pengujian Waktu Enkripsi dan Dekripsi AES-256-CBC 85
Tabel 4. 6 Hasil Pengujian Total Waktu Operasi Unggah dan Unduh 86
Tabel 4. 7 Hasil Pengujian Fungsionalitas Sistem 88
Tabel 4. 8 Hasil Pengujian Performa Sistem 89
Tabel 4. 9 Hasil Pengujian Kemudahan Antarmuka (Usability) 90

DAFTAR ISTILAH DAN SINGKATAN

No	Istilah dan Singkatan	Keterangan
1	API	*Application Programming Interface*
2	Bot API	*Bot Application Programming Interface*
3	AES-256	*Advanced Encryption Standard 256-bit*
4	SHA-256	*Secure Hash Algorithm 256-bit*
5	CBC	*Cipher Block Chaining*
6	IV	*Initialization Vector*
7	UI	*User Interface*
8	*Web UI*	*Web User Interface*
9	REST API	*Representational State Transfer Application Programming Interface*
10	JSON	*JavaScript Object Notation*
11	JWT	*JSON Web Token*
12	SQL	*Structured Query Language*
13	NIST	*National Institute of Standards and Technology*
14	IDC	*International Data Corporation*
15	RAM	*Random Access Memory*
16	SSD	*Solid State Drive*
17	CPU	*Central Processing Unit*
18	HTML	*HyperText Markup Language*
19	CSS	*Cascading Style Sheets*
20	R&D	*Research and Development*
21	MTProto	*Mobile Transport Protocol*
22	PBKDF2	*Password-Based Key Derivation Function 2*
23	CORS	*Cross-Origin Resource Sharing*

24	OWASP	*Open Web Application Security Project*
25	Pyrogram	*Library Python* untuk komunikasi dengan *server* Telegram melalui protokol MTProto
26	TgCrypto	*Library* akselerasi enkripsi native untuk protokol MTProto
27	Gunicorn	*Green Unicorn*
28	WSGI	*Web Server Gateway Interface*
29	I/O	*Input/output*