IMPLEMENTASI *BLOCKCHAIN PADA SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-*3 (SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

SKRIPSI

DISUSUN OLEH

Mhd Fonna Alvy Daulay

2009020004

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2024

IMPLEMENTASI *BLOCKCHAIN* PADA *SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-3 *(SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

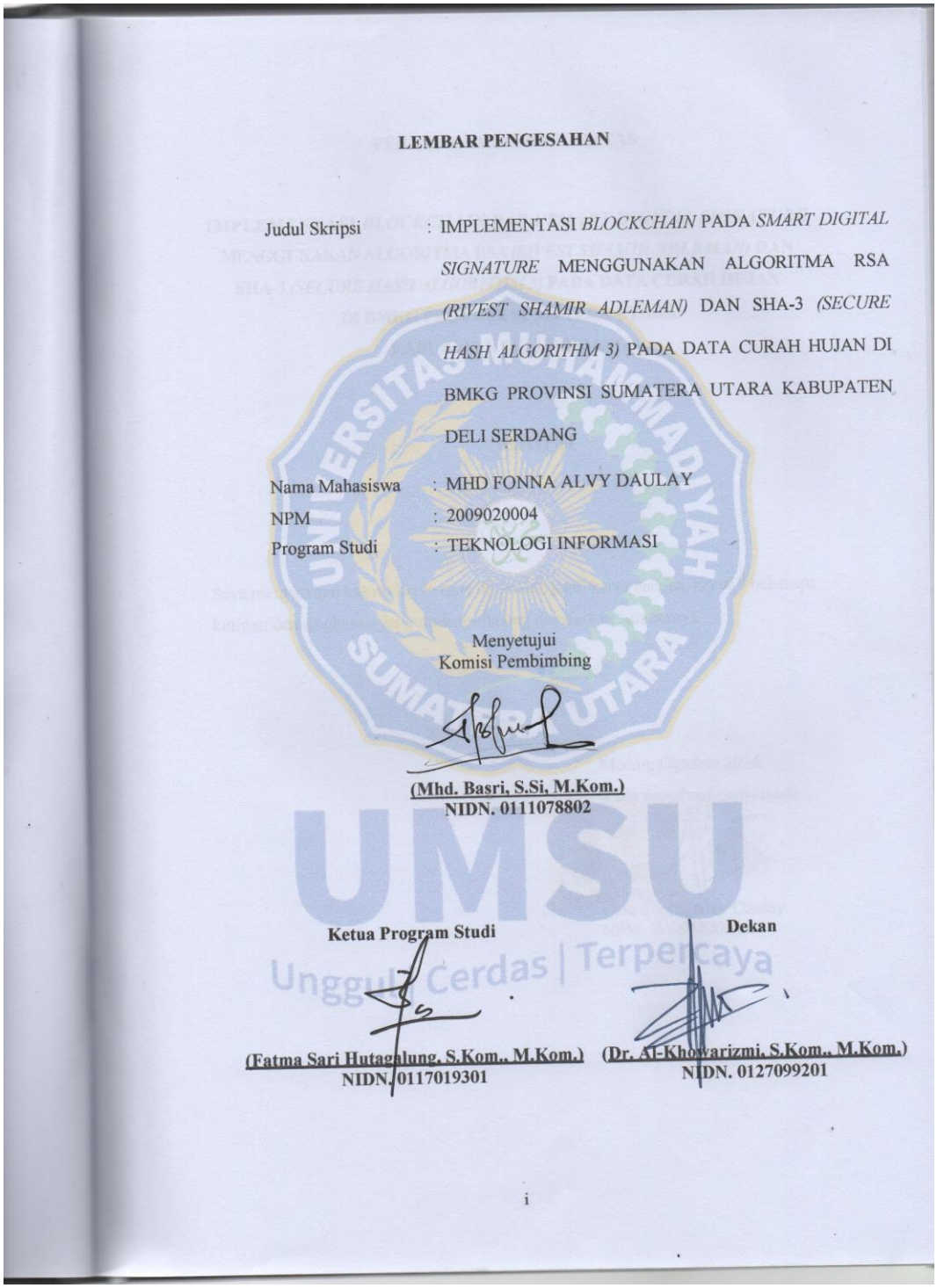
SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Teknologi Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

MHD FONNA ALVY DAULAY
NPM. 2009020004

PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2024

LEMBAR PENGESAHAN



LEMBAR PENGESAHAN

Judul Skripsi : IMPLEMENTASI *BLOCKCHAIN* PADA *SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-3 *(SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

Nama Mahasiswa : MHD FONNA ALVY DAULAY
NPM : 2009020004
Program Studi : TEKNOLOGI INFORMASI

Menyetujui
Komisi Pembimbing

(Mhd. Basri, S.Si, M.Kom.)
NIDN. 0111078802

Ketua Program Studi

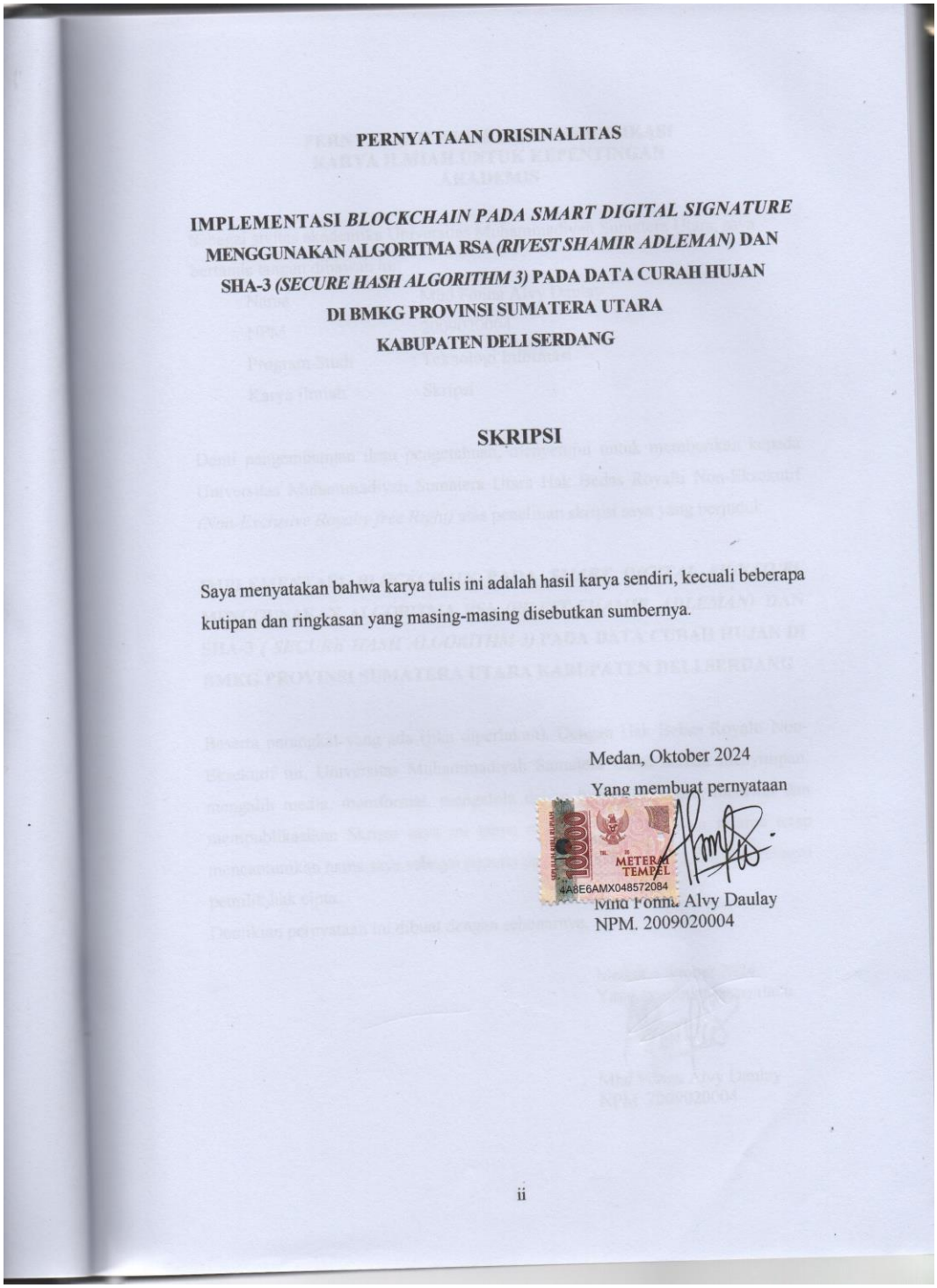
(Fatma Sari Hutagalung, S.Kom., M.Kom.)
NIDN. 0117019301

Dekan

(Dr. Al-Khowarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

i

PERNYATAAN ORISINALITAS



PERNYATAAN ORISINALITAS

IMPLEMENTASI *BLOCKCHAIN PADA SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-3 *(SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, Oktober 2024

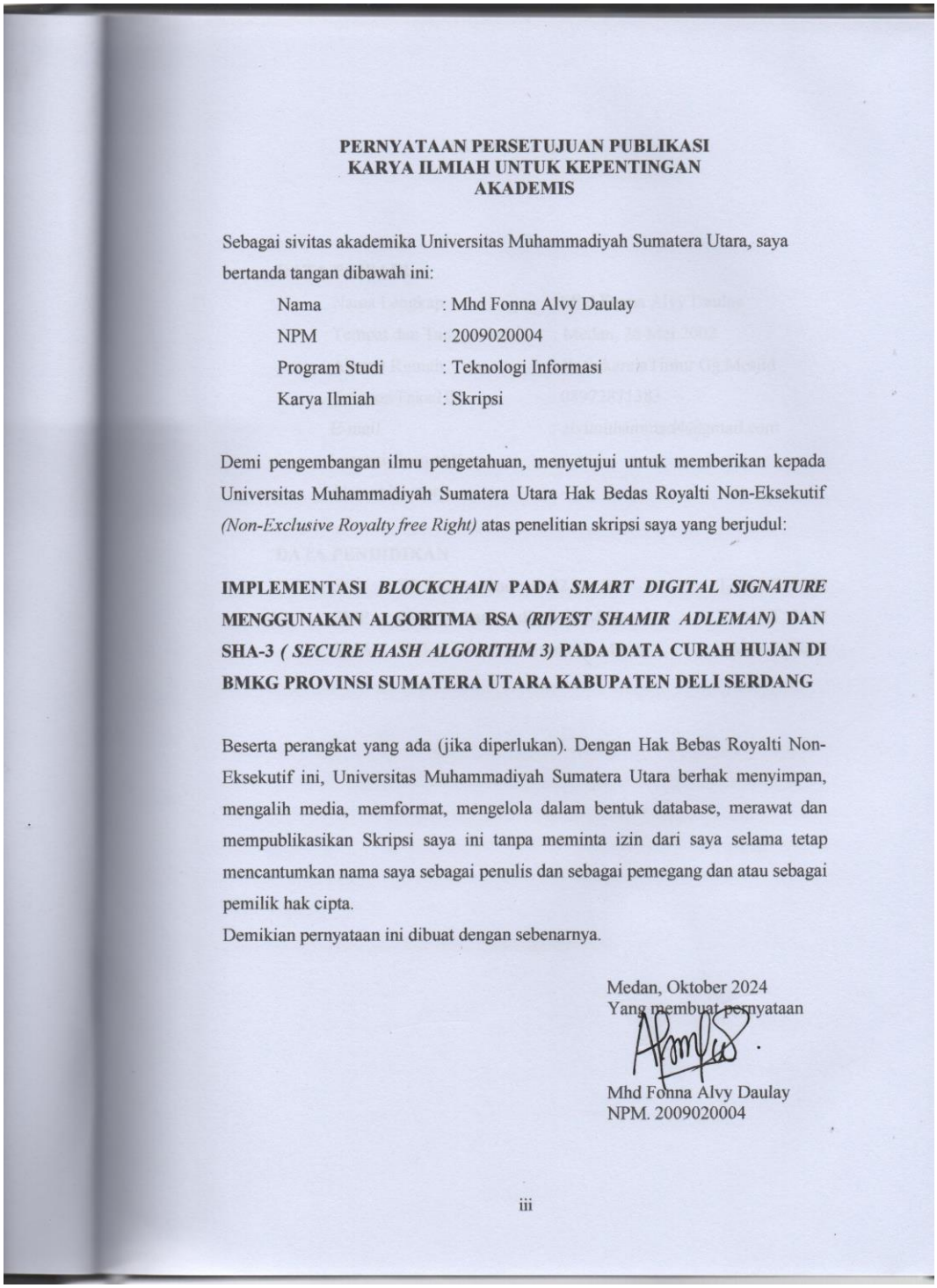
Yang membuat pernyataan

Muhammad Alvy Daulay

NPM. 2009020004

ii

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS



PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Mhd Fonna Alvy Daulay
NPM	: 2009020004
Program Studi	: Teknologi Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

IMPLEMENTASI *BLOCKCHAIN* PADA *SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-3 *(SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.
Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, Oktober 2024
Yang membuat pernyataan

Mhd Fonna Alvy Daulay
NPM. 2009020004

iii

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Mhd Fonna Alvy Daulay
Tempat dan Tanggal Lahir	: Medan, 26 Mei 2002
Alamat Rumah	: JL.SukarelaTimur Gg.Mesjid
Telepon/Faks/HP	: 08972871383
E-mail	: alvimuhammad4@gmail.com
Instansi Tempat Kerja	: -
Alamat Kantor	: -

DATA PENDIDIKAN

SD	: SD Muhammadiyah 02 Medan	TAMAT: 2014
SMP	: SMP Muhammadiyah 07 Medan	TAMAT: 2017
SMA	: SMKS Tritech Informatika Medan	TAMAT: 2020

KATA PENGANTAR

Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Agussani, M.AP., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Fatma Sari Hutagalung, S.Kom., M.Kom. Ketua Program Studi Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
4. Bapak Mhd. Basri, S.Si., M.kom. Sekretaris Program Studi Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
5. Dosen Pembimbing, Bapak Mhd. Basri, S.Si., M.kom.
6. Ayahanda, Bapak Mukhlis Daulay dan Ibunda, Ibu Tri Riandani, selaku orang tua yang telah memberikan kontribusi penuh dalam hidup Ananda semoga segala jerih payah dan usaha yang diberikan dapat Ananda amalkan sehingga ilmu yang didapat
7. Amanda Natasya, Seseorang yang spesial yang juga membantu menyemangati serta selalu mendukung penulis dalam penyusunan skripsi ini.
8. Kerabat kerja penulis dari Mexious Media yang juga membantu dan mendukung penulis dalam penulisan skripsi ini, serta semua pihak lain yang terlibat yang tidak dapat penulis ungkap satu-persatu.

IMPLEMENTASI *BLOCKCHAIN* PADA *SMART DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA RSA *(RIVEST SHAMIR ADLEMAN)* DAN SHA-3 *(SECURE HASH ALGORITHM 3)* PADA DATA CURAH HUJAN DI BMKG PROVINSI SUMATERA UTARA KABUPATEN DELI SERDANG

ABSTRAK

Kemajuan teknologi ini telah memengaruhi hampir semua aspek kehidupan manusia, termasuk komunikasi. Dengan internet, orang dapat berbicara satu sama lain tanpa batasan jarak. Pada penelitian ini berfokuskan bagaimana pengimplementasian blockchain pada smart digital signature, Sistem smart digital signature memungkinkan pengguna mengunduh dan mengunggah dokumen ke sistem, baik yang terenkripsi maupun tidak terenkripsi. Kriptografi kunci publik, terutama tanda tangan digital, dapat digunakan untuk menjawab pertanyaan ini. Digital Signature, juga dikenal sebagai tanda tangan digital, adalah metode otentikasi yang memungkinkan pembuat pesan untuk menyertakan kode. Pada penelitian ini, penulis membahas mengenenai pengimplementasian Blockchain pada smart digital signature, khususnya dengan menggunakan kombinasi antara Algoritma RSA dengan Hash SHA-3, Pada dasarnya kedua algoritma ini masih tergolong kedalam algoritma kriptografi, namun memiliki fungsi yang berbeda beda. Algoritma RSA adalah salah satu algoritma kriptografi paling banyak digunakan untuk membuat tanda tangan digital. RSA menggunakan kriptografi asimetris dengan kunci publik dan privat. Sementara kunci publik digunakan untuk memverifikasi tanda tangan, kunci privat digunakan untuk menandatangani pesan. Algoritma SHA-3 adalah bagian dari keluarga algoritma SHA dan dirancang untuk menambah keamanan dan kinerja dari pendahulunya (SHA-2). Fungsi hash menghasilkan nilai hash tetap (sering disebut hash value atau digest) dari pesan input dengan panjang berapa pun. Dengan menggabungkan kekuatan RSA dalam kriptografi kunci publik dan ketahanan SHA-3 terhadap serangan, maka hasil yang dapat diperoleh dari Implementasi blockchain pada smart digital signature menggunakan algoritm RSA dan SHA-3 dapat memberikan jaminan keamanan yang tinggi untuk aplikasi digital modern.

Kata Kunci: Smart Digital Signature, Algoritma RSA, SHA-3, Blockchain, Kunci Privat, Kunci Publik.

IMPLEMENTATION OF BLOCKCHAIN IN SMART DIGITAL SIGNATURES USING RSA (RIVEST SHAMIR ADLEMAN) AND SHA-3 (SECURE HASH ALGORITHM 3) ON RAINFALL DATA AT BMKG NORTH SUMATERA PROVINCE DELI SERDANG DISTRICT

ABSTRACT

The advancement and development of technology have influenced nearly every aspect of human life, including communication. With the internet, communication can be carried out without distance limitations. This study focuses on the implementation of blockchain in smart digital signatures. A smart digital signature system allows users to download and upload documents within the system, either encrypted or unencrypted. One way to address this is through public key cryptography, specifically digital signatures. A digital signature is a method of authentication that allows the person who created the message to include a code. In this study, the author discusses the implementation of blockchain in smart digital signatures, particularly using a combination of the RSA (Rivest Shamir Adleman) Algorithm with SHA-3 Hashing. Essentially, these two algorithms are classified as cryptographic algorithms but have different functions. RSA (Rivest Shamir Adleman) is one of the most widely used cryptographic algorithms for creating digital signatures. RSA operates on the principle of asymmetric cryptography, where both public and private keys are utilized. The message is signed using the private key, and the signature is confirmed using the public key. SHA-3 (Secure Hash Algorithm 3) is part of the SHA algorithm family and is designed to enhance the security and performance of its predecessor (SHA-2). The hash function generates a fixed hash value (often called a hash or digest) from an input message of any length. By combining the power of RSA in public key cryptography and the resilience of SHA-3 against attacks, the results obtained from the blockchain implementation in smart digital signatures using RSA and SHA-3 algorithms can provide a high level of security assurance for modern digital applications.

Keywords: Smart Digital Signature, RSA Algorithm, SHA-3, Blockchain, Private Key, Public Key.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan dan perkembangan teknologi ini telah memengaruhi hampir semua aspek kehidupan manusia, termasuk komunikasi. Adanya internet memungkinkan orang berbicara satu sama lain tanpa batasan jarak.Pada penelitian ini berfokuskan bagaimana pengimplementasian blockchain pada smart digital signature, Sistem smart digital signature memungkinkan pengguna mengunduh dan mengunggah dokumen ke sistem yang sudah terenkripsi atau tidak terenkripsi. Setelah dokumen diunggah, mereka akan masuk ke layanan penyimpanan cloud, dan setiap file yang masuk atau keluar akan masuk ke server pusat data. (Muhammad Andhika & Gunawan Pria, 2020).

Internet digunakan dalam berbagai bidang, seperti bisnis, perdagangan, industri, dan pemerintahan. Secara umum, informasi yang dikirimkan sangat penting, sehingga keamanan informasi tersebut menjadi hal yang perlu diperhatikan. Salah satu solusi untuk menjawab permasalahan ini adalah dengan menggunakan kriptografi kunci publik, khususnya tanda tangan digital. Tanda tangan digital adalah metode otentikasi yang memungkinkan pengirim pesan untuk menambahkan kode tertentu.

Adapun penjelasan lain mengenai tanda tangan digital adalah mekanisme kriptografi yang memberikan jaminan terhadap keaslian dan integritas pesan digital. Proses ini melibatkan penggunaan algoritma kriptografi untuk membuat tanda tangan yang unik untuk setiap pesan atau dokumen. Tanda tangan digital sering digunakan dalam berbagai aplikasi seperti email, transaksi online, dan

kontrak digital, maupun file dengan beberapa yang berisikan teks, Pada penelitian ini, penulis membahas mengenenai pengimplementasian Blockchain pada smart digital signature, khususnya dengan menggunakan kombinasi antara Algoritma RSA (Rivest Shamir Adleman) dengan Hash SHA-3, Pada dasarnya kedua algoritma ini masih tergolong kedalam algoritma kriptografi, namun memiliki fungsi yang berbeda beda.

RSA (Rivest Shamir Adleman) adalah salah satu algoritma kriptografi paling populer yang digunakan untuk membuat tanda tangan digital. Ini bekerja berdasarkan prinsip kriptografi asimetris dan menggunakan dua jenis kunci—kunci publik dan kunci privat. Sementara kunci publik digunakan untuk memverifikasi tanda tangan, kunci privat digunakan untuk menandatangani pesan.

SHA-3 (Secure Hash Algorithm 3) adalah bagian dari keluarga algoritma SHA dan dirancang untuk menambah keamanan dan kinerja dari pendahulunya (SHA-2). Fungsi hash menghasilkan nilai hash tetap (sering disebut hash value atau digest) dari pesan input dengan panjang berapa pun. SHA-3 memiliki karakteristik utama seperti keamanan, di mana SHA-3 dirancang untuk tahan terhadap berbagai jenis serangan kriptografi seperti collision attacks dan pre-image attacks. Selain itu, kinerja SHA-3 memungkinkan untuk diimplementasikan dengan efisien dalam perangkat keras maupun perangkat lunak.

Dengan menggabungkan kekuatan RSA dalam kriptografi kunci publik dan ketahanan SHA-3 terhadap serangan, maka hasil yang dapat diperoleh dari Implementasi blockchain pada smart digital signature menggunakan algoritm RSA dan SHA-3 dapat memberikan jaminan keamanan yang tinggi untuk aplikasi digital modern. implementasi yang tepat dari teknologi ini sangat penting untuk menjaga

keamanan dalam berbagai aktivitas digital, khususnya untuk tanda tangan digital (digital signature).

1.2 Rumusan Masalah

Penulis mengangkat rumusan masalah yakni “Bagaimana hasil implementasi blockchain pada tanda tangan digital (digital signature) menggunakan algoritma RSA dan SHA-3?

1.3 Batasan Masalah

Agar perancangan Aplikasi tanda tangan digital berbasis GUI (Graphical User Interface) ini dapat diterapkan. Oleh karena itu, batasan masalah yang diambil yakni :

1. Aplikasi berbasis GUI untuk tanda tangan digital (digital signature) menggunakan algoritma RSA dan SHA-3.
2. Aplikasi dapat dijalankan pada Operating System Windows.
3. Pengujian tanda tangan digital (digital signature) menggunakan Algoritma RSA dan SHA-3 dengan beberapa file dengan ekstensi file .xlsx (Microsoft Excel), .txt, .jpg, .png.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yakni untuk mengimplementasikan aplikasi keamanan pesan, filr, teks maupun gambar dengan mengunakan algoritma RSA (Rivest Shamir Adleman) dan SHA-3 (Secure Hash Algorithm 3).

1.5 Manfaat Penelitian

Beberapa manfaat yang dapat diambil dari penelitian ini, diantaranya:

1. Mengurangi dan mencegah dari beberapa kejahatan digital seperti sabotase dan pemalsuan pesan atau data.
2. Mempermudah deteksi keamanan dan kecurangan jika ada tanda tangan digital (digital signature) yang palsu.
3. Menambah wawasan literasi digital pentingnya mengamankan dan menjaga pesan dan data dari beberapa kejahatan digital.

BAB II

LANDASAN TEORI

2.1 Blockchain

Satosi Nakamoto pertama kali membuat blockchain pada tahun 2008 untuk cryptocurrency, tetapi sekarang telah berkembang pesat dan digunakan dalam banyak hal, seperti pencatatan identitas digital, sistem kesehatan, dan rantai pasokan., tanda tangan digital dan termasuk juga proses pencetakan sertifikat (Muhammad Yusup, et al. 2019).

Blockchain berfungsi sebagai protokol yang memungkinkan pihak-pihak untuk mentransfer nilai atau aset tanpa memerlukan pihak ketiga yang dipercaya. Setiap transfer dicatat secara publik dan diverifikasi oleh jaringan, memungkinkan berbagai aset untuk dipertukarkan. Untuk membangun kepercayaan tanpa perantara, semua transaksi dikelompokkan dan disimpan di dalam blok yang diverifikasi secara lokal pada banyak perangkat milik peserta jaringan (node). Setiap blok dilengkapi dengan kode hash, berupa rangkaian angka dan huruf, yang dibuat berdasarkan informasi dalam blok tersebut. Kode hash ini menghubungkan blok-blok tersebut, di mana setiap blok berikutnya merujuk pada hash dari blok sebelumnya. (Ahram T, et al. 2017).

2.2 Tanda Tangan Digital (Smart Digital Signature)

Digital signature atau tanda tangan digital berfungsi sebagai penanda kepemilikan dari suatu dokumen digital. Salah satu cara penerapannya adalah dengan menggunakan teknologi Blockchain. Salah satu upaya dalam memerangi pelanggaran hak cipta dapat dilakukan dengan ilmu blockchain. Blockchain bekerja dengan cara menyimpan data digital di dalam blok-blok yang kemudian dirantai

menjadi satu kesatuan. Tiap blok berisi informasi tertentu dan terkait dengan blok sebelumnya dan sesudahnya. Inilah yang membuat blockchain aman karena data tidak bisa diubah seenaknya. Jika ada yang mencoba mengubah data pada suatu blok, maka semua blok yang terkait harus diubah juga, yang tentunya sangat sulit dilakukan. (Rizky Rahman, et al. 2019).

Tanda tangan digital dibuat secara elektronik dan berfungsi seperti tanda tangan pada dokumen kertas. Tanda tangan digital yang aman tidak dapat diubah oleh penandatangan di kemudian hari dengan mengklaim bahwa tanda tangan tersebut palsu. Dengan demikian, tanda tangan digital dapat menjamin keaslian dokumen yang dikirim secara digital, termasuk jaminan identitas pengirim dan kebenaran isi dokumen tersebut. (Krisna Widatama, et al. 2022).

2.3 Algoritma RSA (Rivest Shamir Adleman)

Rivest Shamir Adleman (RSA) adalah algoritma enkripsi berbasis public key. Algoritma ini sangat cocok untuk tanda tangan digital dan enkripsi, menjadikannya salah satu algoritma terdepan dalam kriptografi public key. RSA telah banyak diterapkan dalam protokol Electronic Commerce dan dipercaya untuk melindungi data dengan menggunakan kunci yang cukup panjang. (Faiz Farhan1 & Dedi Leman, 2023).

RSA bekerja dengan prinsip kriptografi asimetris, yang menggunakan dua kunci berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci publik dapat dibagikan secara bebas, sementara kunci privat harus dirahasiakan. Proses RSA dimulai dengan pembuatan kunci, di mana dua bilangan prima besar, p p dan q q, dipilih secara acak. Kemudian dihitung nilai n n dengan rumus $n = p \times q$ n=p×q, yang digunakan sebagai modulus dalam kedua kunci.

Setelah nilai-nilai tersebut diperoleh, dipilih bilangan bulat e e yang relatif prima terhadap ϕ ( ) ϕ(n), dengan 1 < e < ϕ (n) 1<e<ϕ(n). Langkah selanjutnya adalah menghitung d d, yang merupakan invers modulo dari e e terhadap ϕ (n) ϕ(n), sehingga $e \times d \equiv 1$ (m o d ϕ (n)) e×d≡1(modϕ(n)). Kunci publik terdiri dari pasangan (, n) (e,n), sedangkan kunci privat terdiri dari pasangan (d , n) (d,n). Proses enkripsi pesan dilakukan dengan mengubah pesan M M menjadi bilangan bulat m m sedemikian rupa sehingga $0 \leq m < n$ 0≤m<n. Ciphertext c c kemudian dihitung dengan rumus $c = m\ e$ (m o d n) c=m e (modn). Dekripsi dilakukan dengan menghitung bilangan bulat m m dari ciphertext c c menggunakan kunci privat d d, dengan rumus $m = c\ d$ (m o d n) m=c d (modn). Bilangan m m yang dihasilkan kemudian dikonversi kembali ke pesan asli M M.

Keamanan RSA bergantung pada kesulitan faktorisasi bilangan besar n n menjadi faktor-faktor primanya p p dan q q. RSA tetap aman dengan ukuran kunci yang cukup besar (misalnya, 2048 bit atau lebih). Namun, perkembangan komputasi kuantum dapat mengancam keamanan RSA di masa depan, sehingga penelitian terus dilakukan untuk mengembangkan algoritma kriptografi yang tahan terhadap serangan kuantum.

2.4 Algoritma SHA-3 (Secure Hash Algorithm 3)

SHA dikembangkan oleh National Institute of Standards and Technology (NIST) dan pertama kali diterbitkan sebagai Federal Information Processing Standards (FIPS 180) pada tahun 1993. SHA-3 diciptakan bukan untuk menggantikan SHA-2, melainkan sebagai tanggapan terhadap kekhawatiran NIST atas keamanan fungsi hash seperti MD5, SHA-0, dan SHA-1 yang telah berhasil diretas. Karena kerentanan ini, NIST memutuskan untuk mencari algoritma hash

alternatif yang secara signifikan berbeda dari yang sebelumnya dengan mengadakan kompetisi guna menemukan fungsi hash baru yang lebih aman. (Joshua Allan, *et al*. 2021).

Algoritma SHA-3 mengubah input data menjadi output hash tetap panjang yang disebut nilai hash atau digest. SHA-3 dapat menghasilkan hash dengan panjang yang bervariasi, termasuk SHA3-224, SHA3-256, SHA3-384, dan SHA3-512, yang masing-masing menghasilkan nilai hash dengan panjang 224, 256, 384, dan 512 bit.

Proses hashing dengan SHA-3 dimulai dengan penyerapan (absorbing) di mana input data dipecah menjadi blok-blok kecil, dan setiap blok diproses secara bertahap. Data di-XOR-kan dengan bagian pertama dari status internal (state) yang panjangnya sama dengan ukuran blok. Setelah setiap blok data di-XOR-kan dengan state, sebuah permutasi diterapkan pada state tersebut. Permutasi ini adalah serangkaian transformasi non-linear yang rumit yang membuat data tersebar dengan baik ke seluruh state.

Setelah semua blok input diproses dan permutasi terakhir diterapkan, state akan mengandung hasil akhir dari proses hashing. Nilai hash kemudian diambil dari state ini dalam fase ekstraksi (squeezing). Jika panjang input tidak memenuhi kelipatan tertentu, padding ditambahkan untuk memastikan ukuran blok terpenuhi sebelum proses hashing dimulai.

Struktur spons pada SHA-3 menggunakan dua fase: penyerapan (absorption) dan ekstraksi (squeezing). Dalam fase penyerapan, blok input data di-XOR state

internal dan kemudian permutasi diterapkan. Dalam fase ekstraksi, output hash dihasilkan dari state internal setelah semua data input diproses.

2.5 Penelitian Terkait

Tabel 2.1 Penelitian Terdahulu

No	Judul Penelitian	Metode	Hasil Penelitian	Penulis
1	Smart Digital Signature Berbasis Blockchain Pada Pendidikan Tinggi Menggunakan Metode SWOT	Analisa SWOT	1. SHA-256 digunakan sebagai sistem enkripsi yang diterapkan pada tanda tangan digital untuk memastikan keaslian, memverifikasi validitas, dan melindungi dokumen. 2. Sistem ini dirancang untuk mencegah tindak kejahatan seperti perubahan data, karena bersifat irreversible, artinya data tidak dapat dikembalikan ke bentuk aslinya.	Mohamad Rakhmansyah *et al*, 2021
2	Keamanan Pesan Teks Dengan Metode Enkripsi Dan Dekripsi Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Android	Software Development Life Cycle (SDLC)	1. Aplikasi SMS dengan kriptografi yang telah diimplementasikan ini dapat membantu pengguna menjaga keamanan pesan yang sangat rahasia pada smartphone berbasis Android.	Ari Eko Susanto,2023

No	Judul Penelitian	Metode	Hasil Penelitian	Penulis
3	Implementasi Kriptografi File Ujian Siswa Dengan Metode Rsa Berbasis Website Di Sman 84 Jakarta	Metode Waterfall	1. Aplikasi kriptografi untuk file soal ujian siswa menggunakan metode RSA ini dapat melakukan proses enkripsi dan dekripsi pada file soal yang berisi huruf dan angka. 2. Aplikasi ini memiliki fitur yang hanya dapat diakses oleh admin untuk menambah, mengubah, atau menghapus akun pengguna.	I Gusti Ayu Yogie Andhika Putri & Noni Juliasari, 2022
4	Penerapan Algoritma Enhanced Dual Rivest Shamir Adleman untuk Pengamanan Data	Algoritma Enhanced Dual Rivest Shamir Adleman	1. Membuktikan bahwa proses enkripsi dan dekripsi dengan algoritma kriptografi Enhanced Dual RSA dapat dilaksanakan dengan sukses, memungkinkan data yang terenskripsi dikembalikan ke bentuk pesan asli tanpa ada perubahan jumlah karakter. 2. Penelitian ini mengonfirmasi bahwa hasil perhitungan enkripsi dan dekripsi yang dilakukan secara manual menghasilkan nilai yang sama dengan perhitungan yang dilakukan oleh sistem.	Demonius Sarumaha, *et al*. 2024

No	Judul Penelitian	Metode	Hasil Penelitian	Penulis
5	Aplikasi Enkripsi Data Video Menggunakan Metode RSA Dan Blowfish Berbasis Web	Metode Enkripsi RSA(Rivest Shamir Adleman) Dan Blowfish	1. Penggunaan metode enkripsi RSA (Rivest Shamir Adleman) dan Blowfish berbasis web untuk data video merupakan solusi yang efektif. 2. Menjaga kerahasiaan data video dari akses pihak yang tidak berwenang	Yusmaifany, *et al*. 2024
6	Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) Dan AES (Advanced Encryption Standard) Berbasis Web	Algoritma RSA (Rivest Shamir Adleman) Dan AES (Advanced Encryption Standard)	1. Aplikasi pengaman data ini berhasil mengaplikasikan metode Rivest Shamir Adleman untuk melindungi file atau teks perusahaan. 2. Aplikasi ini dapat menunjukkan bahwa semua file dan teks yang dienkripsi akan berubah menjadi file dengan ekstensi (.Encrypted) yang tidak dapat dibuka tanpa kunci privat. Selain itu, file tersebut dapat dikembalikan ke bentuk aslinya melalui proses dekripsi tanpa mengalami perubahan, dengan tingkat keberhasilan mencapai 100%.	Dika Alfiani Fauzan, *et al*. 2023
7	Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan	Kriptografi Algoritma Rivest Shamir	1. RSA dianggap sebagai algoritma kriptografi yang paling aman saat ini karena belum ditemukan algoritma yang lebih efisien untuk memecahkan sistem keamanannya.	Machsudirwan Alrido, *et al*. 2021

No	Judul Penelitian	Metode	Hasil Penelitian	Penulis
	Data Nilai Siswa Pada SMK Multi Karya Medan	Adleman (RSA)	2. Keamanan sistem semakin terjamin seiring dengan panjangnya kunci yang digunakan. 3. Algoritma ini hanya dapat mengamankan data yang berbentuk teks. 4. Hasil keluaran enkripsi memiliki panjang karakter yang berbeda dari karakter input (plaintext), hal ini disebabkan oleh semakin besar bilangan prima yang digunakan, yang mengakibatkan hasil enkripsi melebihi 256 karakter pada tabel ASCII	
8	Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa	RSA (Rivest Shamir Adleman)	Hasil dari penelitian ini mencakup hal-hal berikut: 1. Perbandingan enkripsi gambar, di mana dari 5 gambar yang diuji, kelima gambar tersebut berhasil dienkripsi. 2. Terdapat perbedaan dalam waktu proses enkripsi setiap gambar (tergantung pada ukuran file yang dienkripsi), serta ukuran file yang telah didekripsi berbeda dari file aslinya.	Alif Khamsyar & Muh. Basri, 2022
9	Implementasi Algoritma Rsa Untuk Perancangan Aplikasi Berbasis Java	Metode Rivest Shamir	1. Proses penyimpanan data penting sekolah menjadi lebih terjaga dan terhindar dari akses oknum yang tidak berwenang.	Muhammad Sugiarto & , Purwanto, 2022

No	Judul Penelitian	Metode	Hasil Penelitian	Penulis
	Desktop Pada Mts Daarul Falah	Adleman (RSA)	2. Waktu untuk enkripsi file adalah 0,16 detik untuk ekstensi .doc, 0,034 detik untuk ekstensi .xls, dan 0,004 detik untuk ekstensi .txt. Sedangkan untuk dekripsi, kecepatan adalah 3,811 detik untuk ekstensi .doc, 1,411 detik untuk ekstensi .xls, dan 0,041 detik untuk ekstensi .txt.	
10	Penerapan Digital Signature Menggunakan Metode RSA Untuk Menvalidasi Keaslian Ijazah SMA Swasta Bina Artha	Metode RSA (Rivest Sahmir Adleman)	1. Penerapan tanda tangan digital dalam menyelesaikan masalah validasi keaslian ijazah di SMA Swasta Bina Artha sangat efektif, hal ini terbukti dengan kemudahan dalam memperoleh informasi ijazah yang diperlukan. 2. Metode RSA dapat digunakan untuk menerapkan tanda tangan digital dalam memvalidasi keaslian ijazah di SMA Swasta Bina Artha. 3. Proses pemodelan penerapan tanda tangan digital yang dirancang dapat dilakukan dengan diawali analisis kebutuhan masalah, kemudian dilanjutkan dengan pemodelan.	Erwin Vasi Waruwu, *et al*. 2021

Dari beberapa Penelitian Terdahulu diatas, penulis dapat menyimpulkan dalam beberapa poin dibawah, diantaranya:

1. Beberapa penelitian diatas belum ada yang menggabungkan antara Algoritma RSA dengan SHA-3, beberapa diantaranya menggunakan Algoritma RSA sebagai algoritma utama dari beberapa penelitian diatas.
2. Algoritma RSA banyak digunakan dalam Kriptografi terutama dalam konteks Blockchain, karena algorita inisangat umum dan terdapat banyak referensinya.

BAB III

METODOLOGI PENELITIAN

3.1 Lingkungan Pengembangan Penelitian

Dalam tahapan lingkungan pengembangan ini, terdapat beberapa hal sebagai pendukung dalam peneliti melakukan implementasi atau membuat aplikasi ini, diantaranya beberapa hal pendukung dalam implementasi penelitian ini akan dijelaskan pada table dibawah

Tabel 3.1 Sistem Pengembangan Penelitian

No	Sistem Pendukung	Sistem Operasi Perangkat
1	Laptop Asus K46CM	Windows 10
2	Visual Studio Code (Code Editor)	Windows 10
3	Mouse (Hardware)	-
4	File/Document pendukung lainnya	-

3.2 Pendekatan Penelitian

Dalam penelitian ini, penulis menggunakan metode penelitian dan pengembangan (R&D). yang mencakup beberapa tahapan, seperti pengumpulan data sampel curah hujan antara Februari hingga Juli 2024 secara open source melalui website resmi lembaga BMKG. pengujian hasil, serta evaluasi.

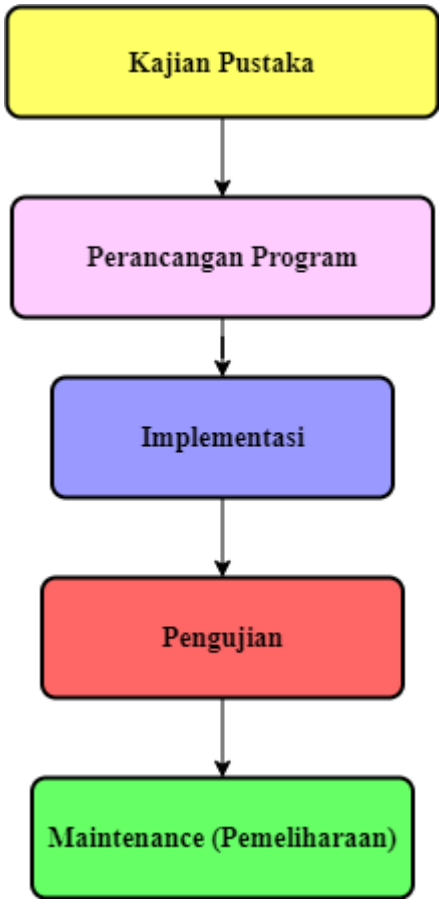
Penelitian ini akan menghasilkan sistem yang berfungsi untuk tujuan tertentu., yaitu untuk menandatangani data digital dengan memanfaatkan teknologi blockchain

Kemudian menggunakan Metode penelitian sekunder , digunakan untuk pengumpulan data yang sudah ada, dalam hal ini data curah hujan dari BMKG. Data sample yang penulis ambil, kemudian dimasukkan ke dalam sistem blockchain untuk proses penandatanganan digital. Dan tidak diperlukan analisis lebih lanjut dari data sample itu sendiri karena hanya berfokus pada teknologi penandatanganan digital.

Selain itu, penelitian ini berkonsentrasi pada penerapan blockchain pada tanda tangan digital (tanda tangan digital) yang menggunakan algoritma RSA dan SHA-3., aplikasi ini berbasis GUI (Graphical User Interface), yang mana aplikasi ini dibuat yang awalnya hanya sebatas dan diakses melalui source code/code editor (Visual Studio Code) dengan cara merunning salah satu file utamannya yaitu main.py, ketika file tersebut dijalankan, maka aplikasi bias dijalankan, namun peneliti berhasil menemukan cara agar bisa lebih efektif menggunakannya yakni merubah/mengconvert file main.py ini menjadi main.exe sehingga jika ingin mengaksesnya hanya tinggal menjalankan file main.exe tersebut, tentu caranya dengan menggunakan salah satu library dari Bahasa pemograman Python yaitu library “pay-to-exe”.

Pada diagram alir diawah terdapat beberapa tahapan penelitian yang diterapkan dalan penelitian ini, tahapan tahapn yang nantinya user akan mengidentifikasi masalah dan tujuan yang ingin diimplementasikan yang berhubungan dengan tanda tangan digital, kemudian user mengumpulkan data-data seperti pesan yang sudah dibentuk kedalam file teks dengan ekstensi .txt, lalu data berupa file gambar dengan ekstensi .png, .jpn,. setelah data dikumpulkan dan diinput ke aplikasinya lalu peran Algoritma RSA mengenkripsi file tersebut

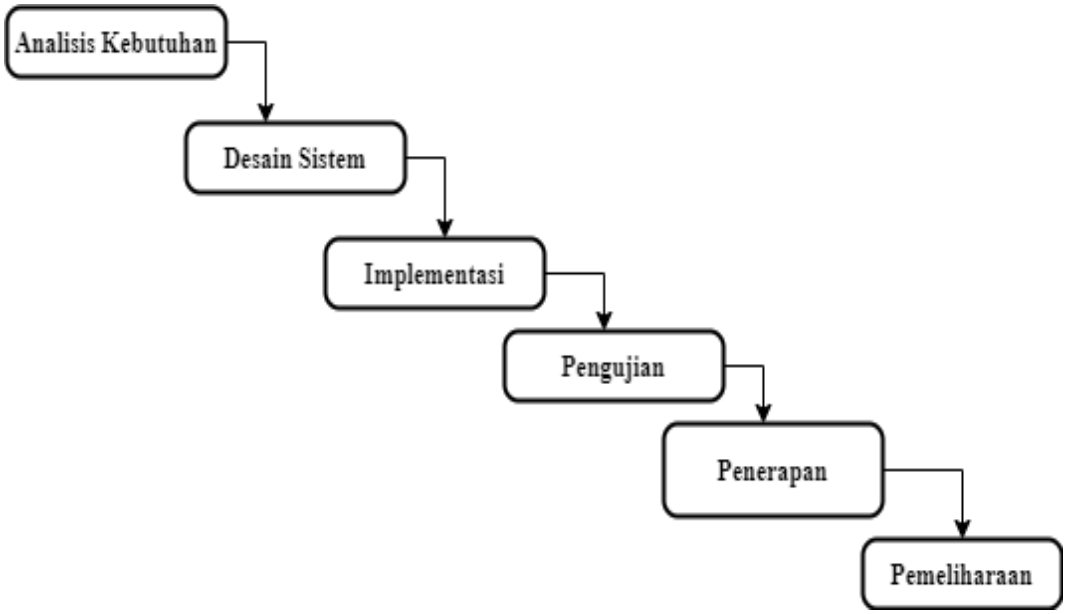
menggunakan kunci public (Public Key) lalu setelah itu file juga akan dideskripsi menggunakan kunci privat (Private Key) setelah itu pesan tersebut sudah berhasil diberikan digital sign (tanda tangan digital), langkah selanjutnya agar file tersebut terhindar dari disalahgunakan, disinilah peran algoritma SHA-3 yang bertujuan memverifikasi file tersebut sehingga file-file tersebut terotentikasi dan valid.



Gambar 3.1 Tahapan Penelitian

3.3 Model Pengembangan Sistem

Model Waterfall digunakan untuk pengembangan sistem., yaitu suatu pendekatan yang sistematis dan berurutan, dimulai dari analisis pengembangan sistem hingga pemeliharaan (maintenance) sistem. Urutan pengembangan perangkat lunak dengan metode Waterfal adalah:



Gambar 3.2 Model Waterfall

1. Analisis Kebutuhan

   Analisis kebutuhan dan pengumpulan seluruh persyaratan untuk sistem tanda tangan digital menggunakan algoritma RSA dan SHA-3, mencakup evaluasi fungsi dan kinerja kedua algoritma tersebut dalam penerapan tanda tangan digital.

2. Desain Sistem

   Menyusun desain sistem berdasarkan kebutuhan yang telah dianalisis. Ini mencakup arsitektur sistem, desain basis data, dan desain algoritma yang mengintegrasikan RSA dan SHA-3.

3. Implementasi

mengembangkan sistem berdasarkan desain yang telah dibuat. Proses ini mencakup pengkodean modular elemen dari algritma RSA dan SHA-3 untuk memastikan bahwa semua komponen bekerja dengan baik.

4. Pengujian

   Melakukan pengujian menyeluruh pada sistem untuk memastikan bahwa setiap komponen beroperasi sesuai spesifikasi. Pengujian mencakup unit testing untuk mengevaluasi sejauh mana algoritma RSA dan SHA-3 dapat bekerja dengan tepat dalam memproses beberapa file yang akan dieksekusi.

5. Penerapan

   Menerapkan sistem yang telah diuji ke lingkungan produksi. Ini mencakup instalasi, konfigurasi data jika diperlukan, sehingga sistem siap digunakan oleh use

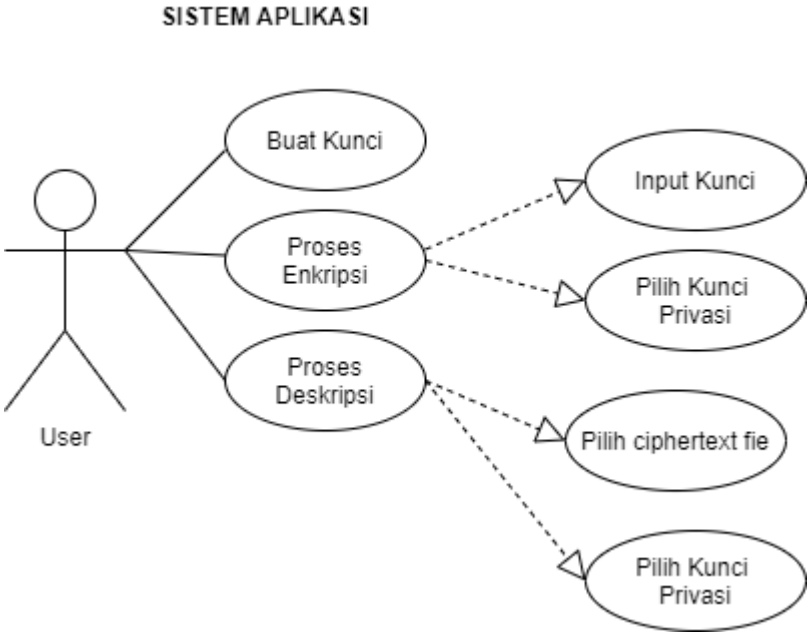
6. Pemeliharaan

   Melakukan pemeliharaan berkelanjutan untuk memperbaiki bug, melakukan peningkatan, dan memastikan sistem tetap berfungsi dengan baik seiring waktu.

3.4 Perancangan Sistem

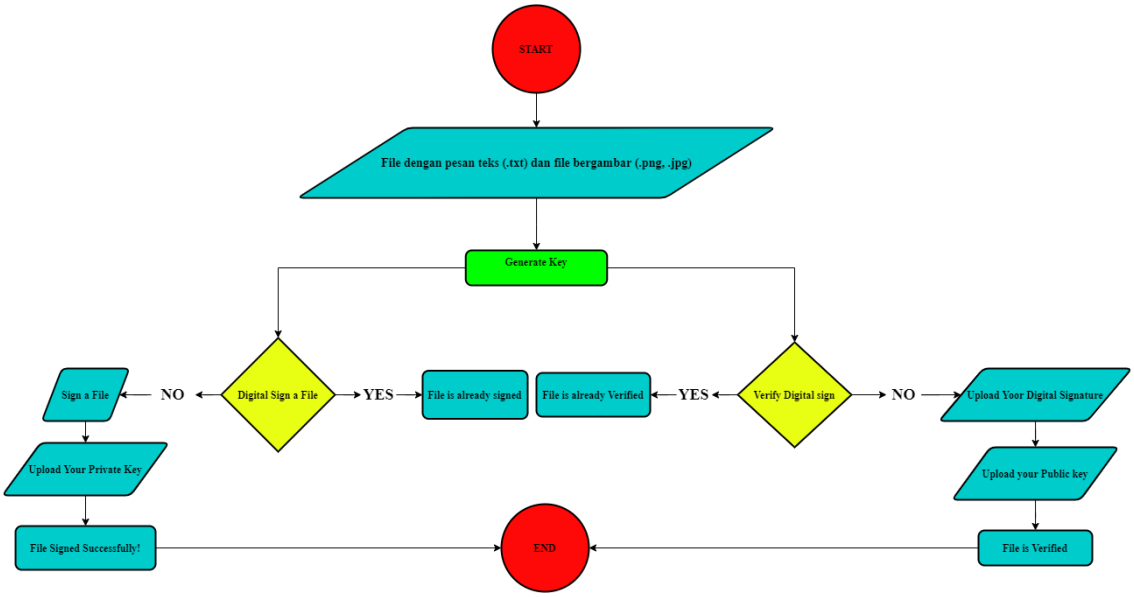
3.4.1 Use Case Diagram Sistem

Diagram use case Unified Modelling Language (UML) menunjukkan bagaimana sistem dan pengguna berinteraksi satu sama lain. Gambar berikut menunjukkan cara sistem aplikasi berinteraksi dengan pengguna, termasuk pembuatan kunci dan proses enkripsi dan dekripsi.



Gambar 3.3 Use Case Diagram Sistem

3.4.2 Flowchart Sistem



Gambar 3.4 Flowchart Sistem Aplikasi

Penjelasan mengenai beberapa alur diagram/flowchart tersebut diantaranya:

1. Generate Key

   Generate key adalah langkah pertama dalam menghasilkan kunci publik dan privat, proses yang terjadi didalamnya bisa dilihat pada gambar dibawah ini:

```
button1 = ttk.Button(start_menu, text="Generate Key", command=lambda: generate_keypair()).pack(pady=10)
```

Gambar 3.4 Tombol Generate Key

Diatas adalah sourcecode tombol dari “Generate Key” ketika tombol ini diklik akan menghasilkan kunci public dan privat.

```
25  def generate_prime_number():
26      while True:
27          result = random.randint(0, 100000000)
28          if is_prime(result):
29              return result
30
31
32  def generate_keypair():
33      p = generate_prime_number()
34      q = generate_prime_number()
35
36      while p == q:
37          q = generate_prime_number()
38          q = generate_prime_number()
```

Gambar 3.5 Proses Generate Key

Diambil beberapa kesimpulan diantaranya:

- generate_prime_number()

  Menghasilkan bilangan prima secara acak adalah tujuan dari fitur ini.

- (while True): Perulangan yang akan terus berulang sampai menemukan bilangan prima. Menghasilkan Bilangan Acak.

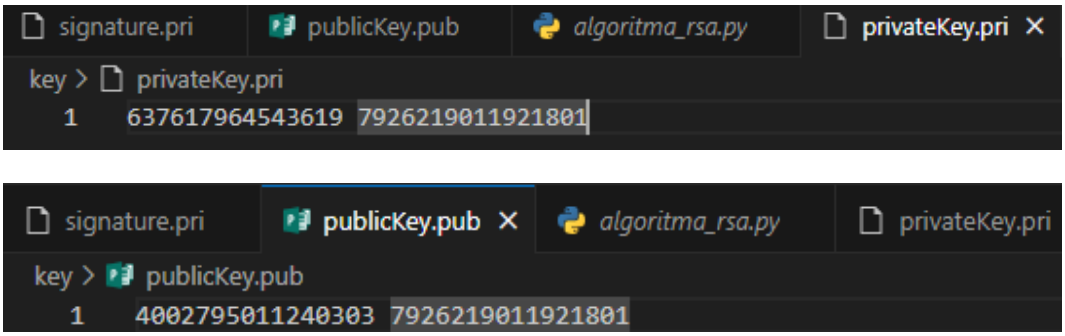
- (random.randint(0, 100000000)): Menghasilkan bilangan acak antara 0 dan 100.000.000.

- (is_prime(result)): Jika bilangan yang dihasilkan adalah bilangan prima (berdasarkan fungsi is_prime yang tidak terlihat di kode ini tapi diasumsikan ada), maka, Mengembalikan Bilangan Prima (return result): Bilangan prima tersebut dikembalikan dan loop berhenti.

- generate_keypair()

  Untuk mendapatkan dua bilangan prima (p dan q), gunakan fungsi generate_prime_number() dua kali.

Memastikan p dan q Berbeda (while p == q): Jika p dan q sama, maka loop while akan dijalankan. Di dalam loop ini, q dihasilkan kembali dua kali. Ini mungkin kesalahan karena seharusnya cukup menghasilkan sekali.



Gambar 3.6 Hasil Kunci Publik dan Kunci Privat Setelah Di Generate

2. Digital sign a file

   Dalam tahapan ini ada beberapa tahapan selanjutnya, diantaranya:

   - Sign a File: Upload file pesan text (.txt) atau file bergambar (.png, .jpg) untuk ditanda tangani
   - Upload Your Private Key: Mengupload private key yang sebelumnya sudah di generate di awal
   - File Signed Successfully: File yang diupload tadi dan diberikan kunci privat telah berhasil ditanda tangani dan berhasil dienkripsi dan deskripsi
   - File is Already Signed: Notifikasi ini akan muncul ketika user menginput file yang sudah ditanda tangani sebelumnya.

3. Verify Digital Sign

   Tahapan ini bertujuan untuk memverifikasi file yang sudah ditanda tangani sebelumnya untuk diuji file tersebut apakah valid dan agar tidak bias disalahgunakan user lain.

4. Upload Your Digital Signature

Ini adalah tahapan dimana user harus input file yang sebelumnya sudah ditanda tangani untuk di verifikasi.

5. Upload Your Private Key

   Ini adalah tahapan dimana user menginput kunci private yang sudah degenerate diawal pemrosesan tadi.

6. File is Verified

   Ini adalah pemberitahuan jika sudah semua langkah-langkah dilakukan, maka file yang sudah diberi tanda tangan digital sudah terotentikasi dan valid, tidak bias disalah gunakan, file berhasil diverifikasi dan mendapatkan hash hash unik.

7. File is Already Verified

   Pemberitahuan ini jika user sudah menginput file yang sudah diverifikasi.

3.5 Algoritma RSA (Rivest Shamir Adleman)

RSA adalah algoritma kunci publik yang paling dikenal dan memiliki berbagai aplikasi.(Rinaldi Munir, 2023) Algoritma yang diciptakan oleh tiga ilmuwan dari MIT (Massachusetts Institute of Technology) Ronald Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976 dikenal sebagai RSA. Kesusahan dalam memproses bilangan bulat besar menjadi komponen prima adalah dasar keamanan RSA.

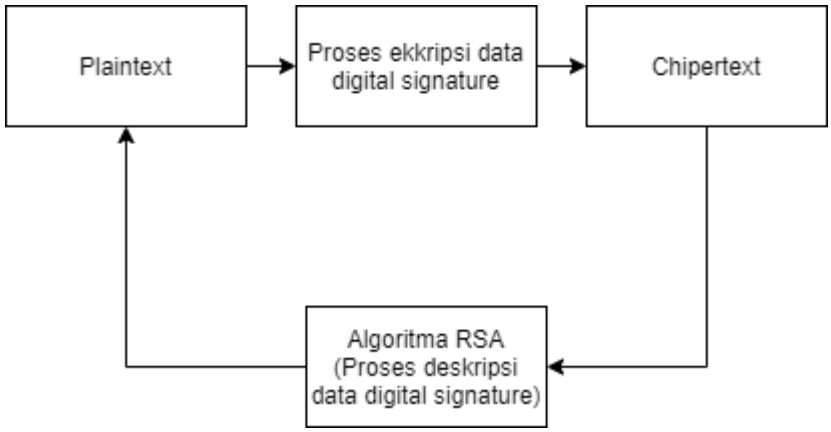
Algoritma RSA memiliki beberapa property dengan berbagai kriteria, diantaranya:

A. Properti Algoritma RSA

Tabel 3.2 Properti Algoritma RSA

No	Properti Algoritma	Kriteria
1	p dan q Bilangan prima	Rahasia
2	n = p □ q	Tidak Rahasia
3	□(n) = (p – 1) (q – 1)	Rahasia
4	e (kunci enkripsi)	Tidak Rahasia
Syarat: PBB(e, □(n)) = 1 , PBB = pembagi bersama terbessar = gcd		
6	d (kunci dekripsi)	Rahasia
d dihitung dari d □ e -1 mod (□(n))		
7	m (plainteks)	Rahasia
8	c (cipherteks)	Tidak Rahasia

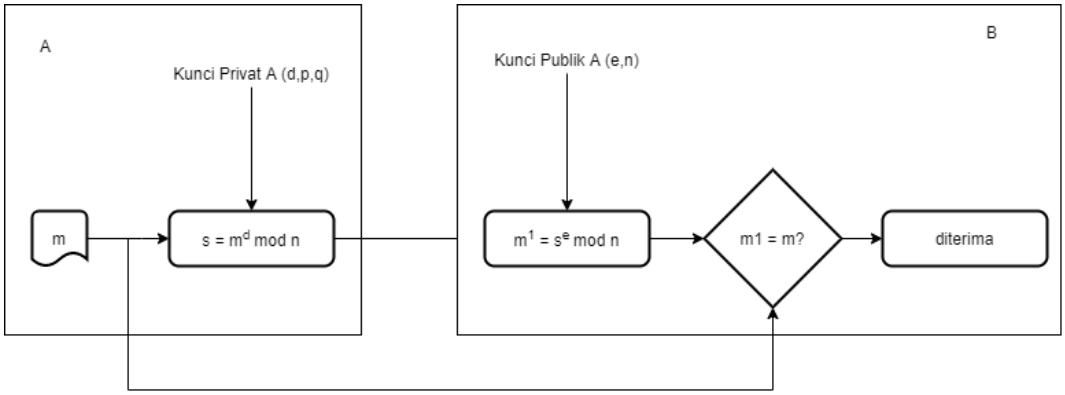
B. Skema Metode Rivest Shamir Adleman (RSA)



Gambar 3.7 Skema Algoritma RSA

Menurut Muhammad Sugiarto & Purwanto (2022), Enkripsi (teks biasa) dan dekripsi (teks sandi) adalah dua kunci algoritma RSA. Di atas, telah dijelaskan skema Algoritma RSA mulai dari proses enkripsi teks biasa hingga dekripsi teks sandi.

C. Skema Pembangkitan Kunci Algoritma RSA (Rivest Shamir Adleman)



Gambar 3.8 Skema Pembangkin Kunci Algoritma RSA

Di dalam sebuah referensi jurnal oleh Fifin Sonata *et al*. 2021, Metode RSA digunakan untuk membuat tanda tangan digital. Sistem kriptografi RSA dapat disesuaikan untuk mendukung skema tanda tangan digital ini, yang terdiri dari beberapa langkah, seperti

1. Pembangkit Kunci

Fungsi pembangkit kunci ini menggunakan objek RSA, yang merupakan representasi dari sistem kriptografi asimetrik RSA, dan mengembalikan hasil dari proses pembangkit kunci. Algoritma ini bekerja dengan cara yang sama seperti sistem kriptografi RSA, menghasilkan kunci publik Kpublik = (e,n) dan kunci privat Kprivat = d.

Algoritma Pembangkit Kunci RSA:

$n = p \times q$

$\phi(n) = (p - 1) \times (q - 1)$

Pilih e yang memenuhi $\gcd(e, \phi(n)) = 1$

$d = e^{-1} \bmod \phi(n)$

Kunci Publik (K_{Publik}) = (e, n), Kunci Privat (K_{Privat}) = d

Keterangan:

p, q : Merupakan bilangan prima

n : Adalah modulus yang digunakan

e : Merupakan eksponen publik atau eksponen enkripsi

d : Merupakan eksponen pribadi atau eksponen dekripsi

Nilai p dan q harus masing-masing 512 bit, sehingga ukuran n 1024 bit. Dengan asumsi bahwa p dan q adalah bilangan prima, φ(n) = (p-1) x (q-1). Selanjutnya, temukan secara acak sebuah bilangan bulat e dari (n) yang memenuhi gcd(e, φ(n)), sehingga e menjadi generator pada Zφ(n). Selanjutnya, algoritma pembangkit kunci RSA menemukan d sebagai invers perkalian e dalam (n). Terakhir, algoritma ini menetapkan kunci publik (e, n) dan kunci privat yang tetap dirahasiakan (d).

2. Algoritma Sign (Tanda Tangan)

Pesan M, kunci privat, dan kunci publik RSA dapat dimasukkan ke dalam algoritma tanda dengan perhitungan eksponensial modular.

Algoritma tanda tangan dalam skema tanda tangan digital RSA:

Input : M, Kprivat = d, K publik = (e,n)

Output : *ρ {signature}*

ρ : M^d mod n3.

3. Algoritma Verify (Verifikasi)

B menerima pasangan *(M, ρ)* dari A, kemudian B memverifikasi *(M, ρ)* dengan menjalankan algoritma Verify yang dijelaskan dalam langkah-langkah berikut:

Algoritma Verify skema tanda tangan digital RSA

Input : *(M, ρ)*, Kpublik = *(e, n)*

Output : diterima

M' = *ρe* mod n

If *M* = M', then

diterima = true l

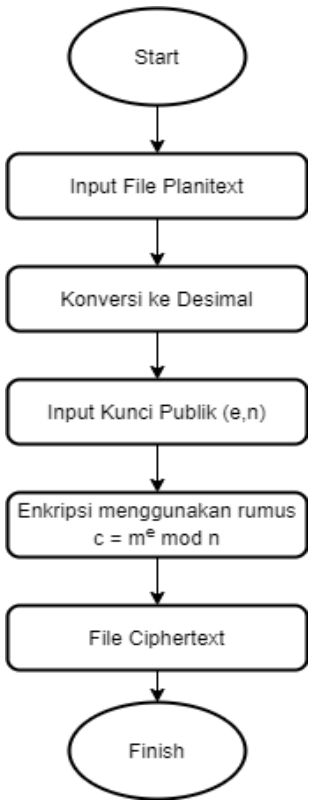
else

diterima = false

end if

D. Enkripsi

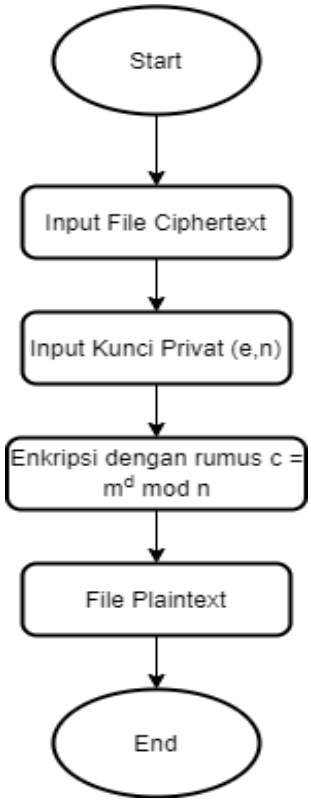
Pada gambar dibawah ini merupakan proses Enkripsi dari system yang dibuat



Gambar 3.9 Proses Enkripsi

E. Deskripsi

Gambar berikut menunjukkan proses enkripsi sistem yang dibuat.



Gambar 3.10 Proses Deskripsi

F. Keamanan Algoritma RSA

Keamanan algoritma RSA bergantung pada tingkat kesulitan dalam memfaktorkan bilangan bulat n menjadi dua faktor prima (p dan q), di mana $n = p \times q$. Setelah n berhasil difaktorkan menjadi p dan q, nilai $\phi(n) = (p - 1) \times (q - 1)$ dapat dihitung. Selain itu, kunci dekripsi d dapat dihitung karena kunci enkripsi e publik (bukan rahasia). berdasarkan kongruensi $ed \equiv 1 \pmod{\phi(n)}$.

G. Contoh Parameter Algoritma RSA

Parameter modulus n algoritma RSA memiliki 1024 bit, atau 300 digit desimal, sementara bilangan prima p dan q masing-masing memiliki panjang sekitar 154 digit desimal.

Tabel 3.3 Contoh Parameter Algoritma RSA

n	11929413484016950905552721133125564964460656966152763801206748 19549430568511503338063159570377156202973050001186287708466899 69112892212245457118060574995989517080042105263427376322274266 39311619351783957077350563223159668112192733747397322031251259 90612313222509455062600665575382385175753906 21262940383913963
p	10933766183632575817611517034730668287155799984632223454138745 67112127345628767000829084330287552127497024531459322294612906 453835858101861553982 8479146469
q	10910616967349110231723734078614922645337060882141748968209834 22513897601117999339429981015973690446855402170828982439655341 218051482799644484543 8176099727

Sumber: Rinaldi Munir (Kriptografi dan Coding).

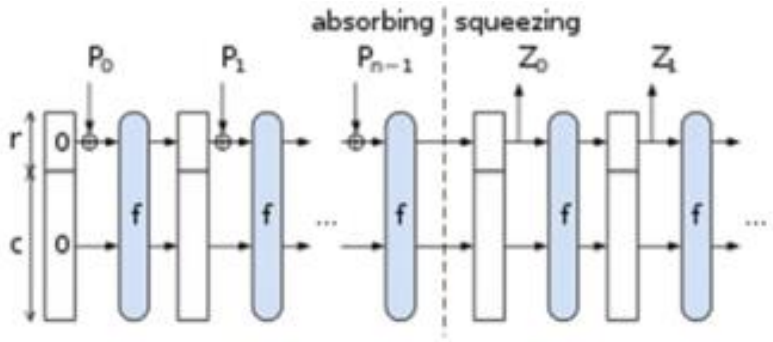
Jika panjang nilai n hanya 256 bit atau kurang, maka RSA hanya akan aman dalam beberapa jam., n dapat difaktorkan menggunakan komputer PC dan program bebas akses. Beberapa ratus komputer sudah cukup untuk memfaktorkan n dengan panjang 512 bit atau kurang. Saat ini, kunci RSA yang dianggap aman memiliki panjang n yang lebih besar dari 1024 bit.

3.6 Algoritma SHA-3 (Secure Hash Algorithm 3)

SHA-3 mengimplementasikan struktur sponge dalam proses hashing, yang melibatkan dua tahap utama: penyerapan (absorbing) dan ekstraksi (squeezing). Proses ini dimulai dengan data input yang kemudian diubah menjadi output hash dengan panjang tetap.

Desain SHA-3 menggunakan konstruksi spons, di mana spons menyerap data. Pada langkah ini, blok pesan di-XOR-kan dengan status dan kemudian diubah secara keseluruhan dengan fungsi permutasi f. Selanjutnya, hasil diperas, di mana

fungsi transformasi status f digunakan untuk mendapatkan blok keluaran dari subset status yang sama. (Morita Puspita Sari, 2021).



Gambar 3.11 Konstruksi Algoritma SHA-3

Struktur spons fungsi hash terdiri dari dua tahap utama: Pi adalah input, dan Zi adalah output hash. Kapasitas c yang tidak digunakan harus dua kali lipat resistansi terhadap benturan atau serangan preimage yang diinginkan. Secara umum, pembuatan spons terdiri dari dua tahapan berikut:

1. Fase absorbing, yaitu tahap di mana setiap pecahan input di-XOR-kan dan kemudian diproses melalui fungsi f dengan bagian bitrate dari state.
2. Fase squeezing, yaitu tahap untuk menghasilkan output dengan menggabungkan sejumlah bit tertentu dari hasil fungsi f, sehingga jumlah bit yang digabungkan sesuai dengan jumlah bit yang diinginkan.

Perhitungan logika hash SHA-3 menggunakan state dengan c = 25W-r bit state, yang tidak dipengaruhi oleh input atau output, dan tanpa stack dalam proses logikanya. Namun, usulan SHA-3 secara konservatif menetapkan c = 2n, di mana n adalah ukuran output hash. Oleh karena itu, nilai r, yang merupakan jumlah bit pesan yang diproses per blok permutasi, bergantung pada ukuran output hash. Untuk ukuran hash 224, 256, 384, dan 512, nilai r tersebut adalah 1152, 1088, 832, atau 576, yang berarti 144, 136, 104, dan 72 byte.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pendahuluan

Bab ini berbicara tentang Implementasi Blockchain Pada Smart Digital Signature Menggunakan Algoritma RSA Dan Sha-3, tentang bagaimana cara kerja sistem berjalan serta komponen apa saja yang digunakan, Bab ini juga akan menjelaskan fungsi beberapa tombol sistem., seperti kegunaan tombol generate key, serta dan lainnya.

Selain itu pengimplementasian kinerja Algoritma RSA dan SHA-3 dalam memproses enkripsi dan deskripsi data yang diinput sehingga menghasilkan block kunci yang berfungsi untuk keamanan data.

4.2 Komponen Pendukung Sistem

4.2.1 Penjelasan Bahasa Pemograman Yang Digunakan dan Komponen dalam Sistem

Sistem yang dikembangkan dalam pembahasan penelitian ini menggunakan Bahasa pemograman Python dengan menggunakan Algoritma RSA dan SHA-3, serta menggunakan text editor Visual Studio Code untuk membuat dan menjalankan programnya, beberapa komponen yang terlibat dalam pengimplementasian blockchain pada Smart Digital Signature ini ia

1. Bahasa Pemograman Python

Dalam Penelitian ini penulis menggunakan Bahasa pemograman Python sebagai program yang berguna untuk menjalankan dan mengoperasikan system yang dibuat dalam penelitian ini, berdasarkan beebrapa referensi, Bahasa pemograman Python ini banyak digunakan khususnya sebagai pengimplementasian blockchain pada smart digital signature, dengan itu penulis menggunakan Bahasa pemograman ini dalam penelitian kali ini, dengan memanfaatkan library yang tersedia yang sangat berguna membantu kinerja penulis, salah satu library yang penulis gunakan yaitu “Py to exe” yang mana library ini berguna untuk mengconvert program menjadi kedalam bentuk desktop dan bias dioperasikan dalam bentuk desktop.

2. VS Code (Visual Studio Code)

Adalah editor teks kode sumber gratis dan terbuka yang dikembangkan oleh Microsoft.yang bersifat terbuka dan gratis, dikembangkan oleh Microsoft. Diluncurkan pertama kali pada tahun 2015, VS Code dengan cepat meraih popularitas di kalangan pengembang perangkat lunak karena kemampuannya yang ringan, cepat, dan dilengkapi dengan berbagai fitur.Berikut adalah beberapa fitur utama dari Visual Studio Code:

1. Dukungan Banyak Bahasa Pemrograman

   VS Code mendukung berbagai bahasa pemrograman seperti Python, JavaScript, TypeScript, C++, Java, PHP, dan banyak lagi. Ini memungkinkan pengembang untuk bekerja dengan berbagai bahasa dalam satu editor. (Dalam Penelitian ini, Penulis menggunakan Bahasa pemograman Python).

2. Debugging

   VS Code memiliki alat debugging yang kuat yang mendukung debugging kode langsung di dalam editor. penulis dapat menjalankan, menghentikan, dan melacak variable.

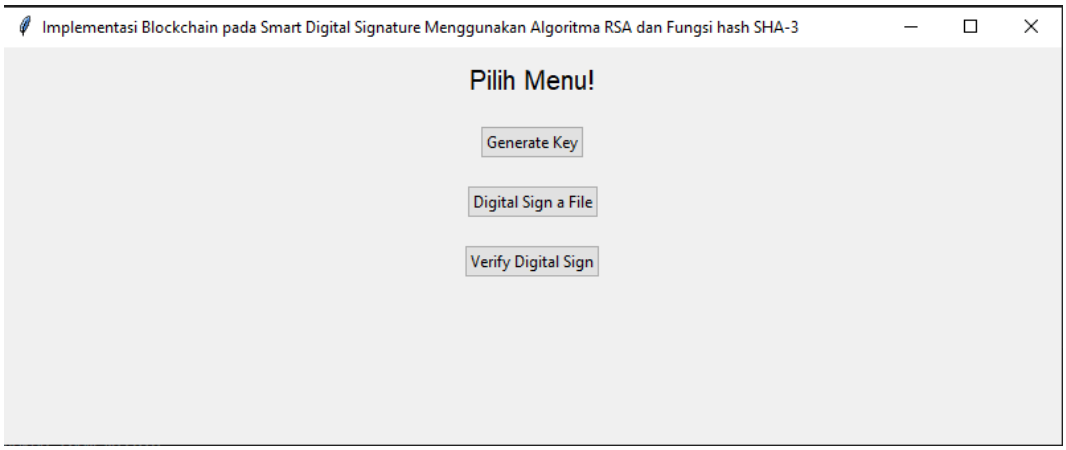
3. Pengelolaan Versi (Version Control)

   VS Code terintegrasi dengan Git dan sistem pengendalian versi lainnya, memungkinkan penulis untuk mengelola repositori, melakukan commit, push, pull.

4. Ekstensi

   Salah satu kekuatan terbesar dari VS Code adalah kemampuannya untuk diperluas. Penulis dapat menambahkan ekstensi yang mendukung berbagai bahasa, alat pengembangan, tema, dan fungsionalitas.

4.2.2 Tampilan Antarmuka Sistem Aplikasi

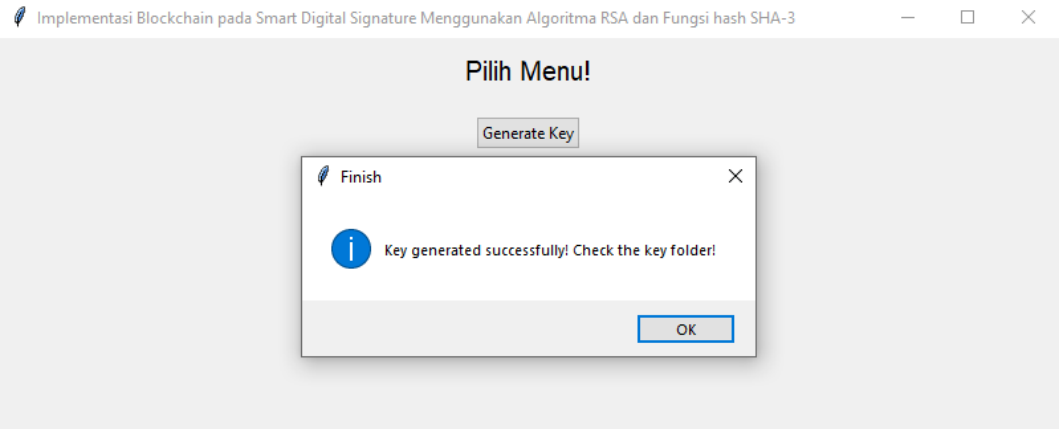


Gambar 4.1 Tampilan Antarmuka Sistem Aplikasi

Gambar diatas merupakan tampilan awal pada saat mengakses aplikasinya, terdapat 3 Tombol yang memiliki kegunaannya masing masing, diantaranya:

1. Tombol Generate Key

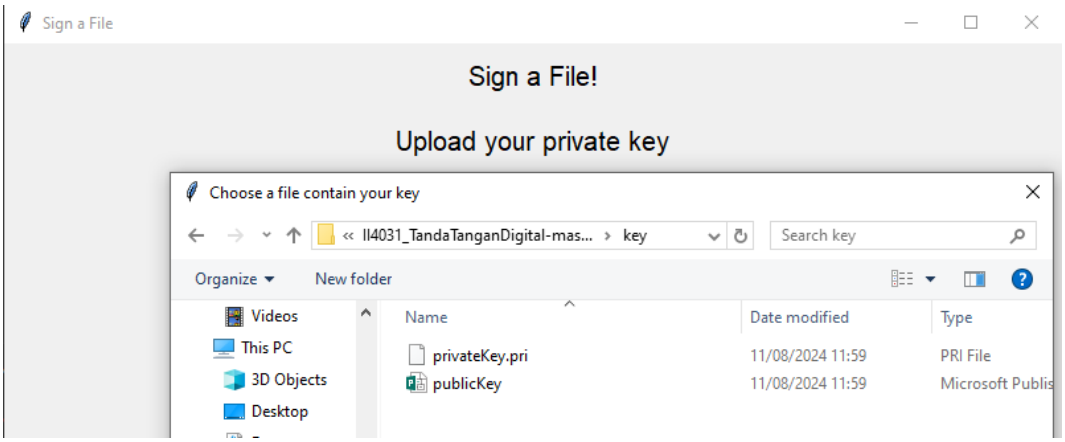
   Dilihat pada gambar diawah, tombol ini memiliki fungsi untuk mengenerate Key/Kunci yang akan digunakan untuk menanda tangani file/data yang ini di enkripsi.



Gambar 4.2 Proses Generate Key

2. Tombol Digital Sign a File

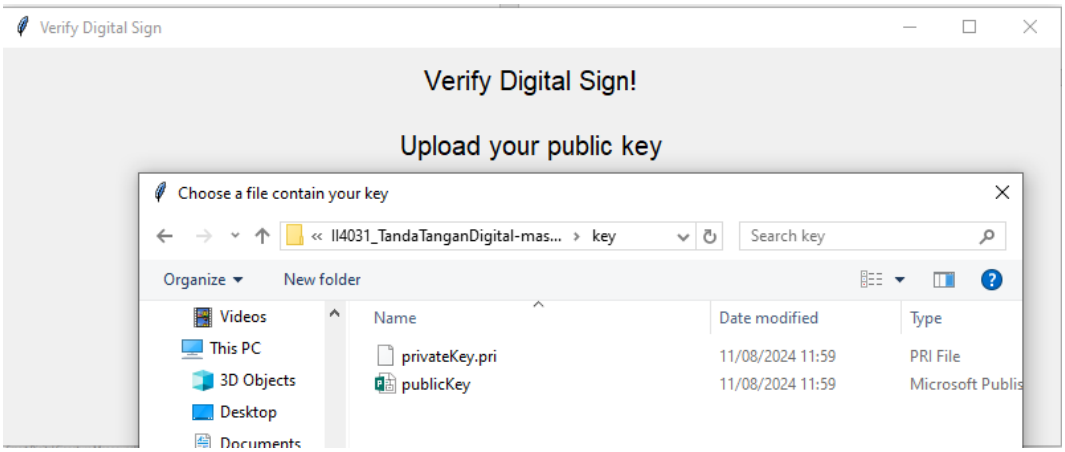
   Pada gambar dibawah, tombol ini memiliki fungsi untuk menginput data/file yang ingin diberikan tanda tangan, serta mengupload private key yang sudah digenerate sebelumnya.



Gambar 4.3 Proses memberikan tanda tangan dan kunci private file/data

3. Tombol Verify Digital Sign

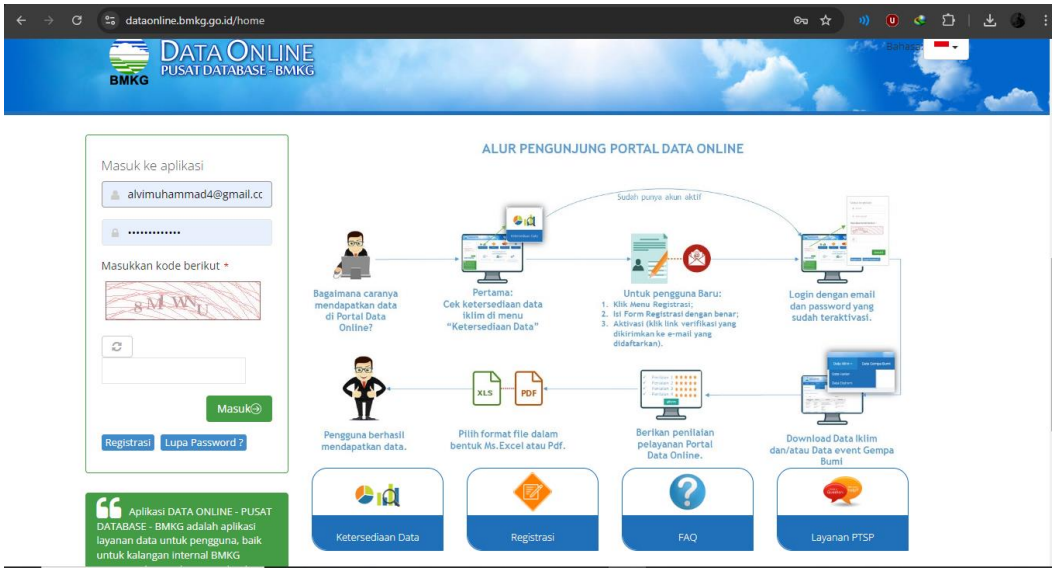
   Pada gambar dibawah, tombol ini memiliki fungsi untuk memverifikasi file/data yang mana saja yang sudah ditanda tangani ataupun belum, bergunfsi untuk memeriksa apakah data/file tersebut sudah diberikan tanda tangan atau belum, jika sudah maka data tersebut langsung di verifikasi, dan tombol ini juga berfungsi untuk mengupload kunci publik



Gambar 4.4 Proses Verifiksi File

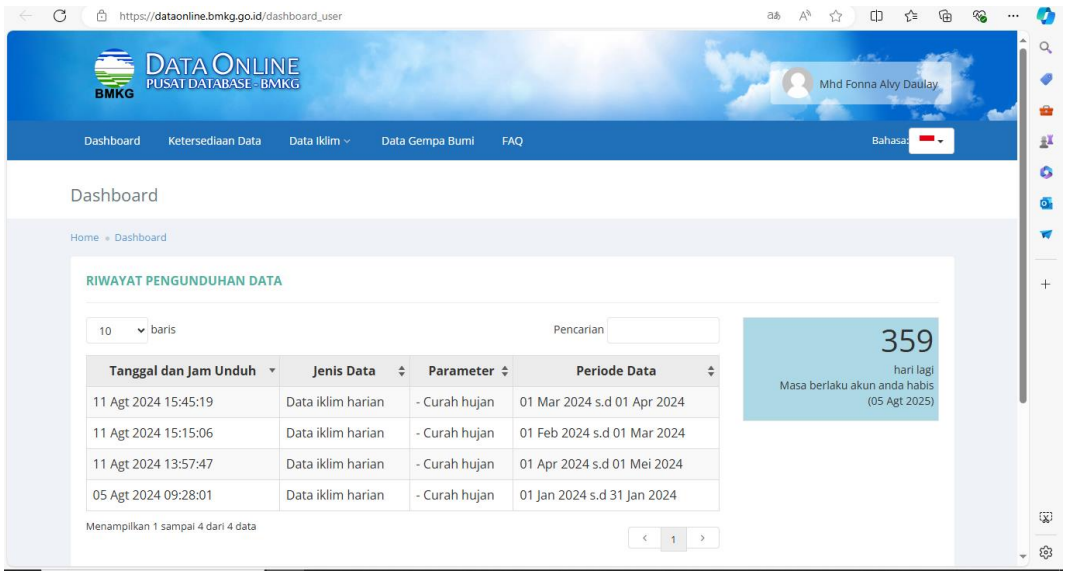
4.3 Pembahasan dan Sumber Sample Data

Pada pembahasan kali ini penulis mengambil data sample curah hujan yang didapat langsung dari website resmi lembaga Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) secara Open Source (Free Akses), untuk Provinsi Sumatera Utara, Kabupaten Deli Serdang, tepatnya pada Stasiun Klimatologi Sumatera Utara dengan rentang waktu 1 Februari – 1 Juli 2024 (5Bulan).



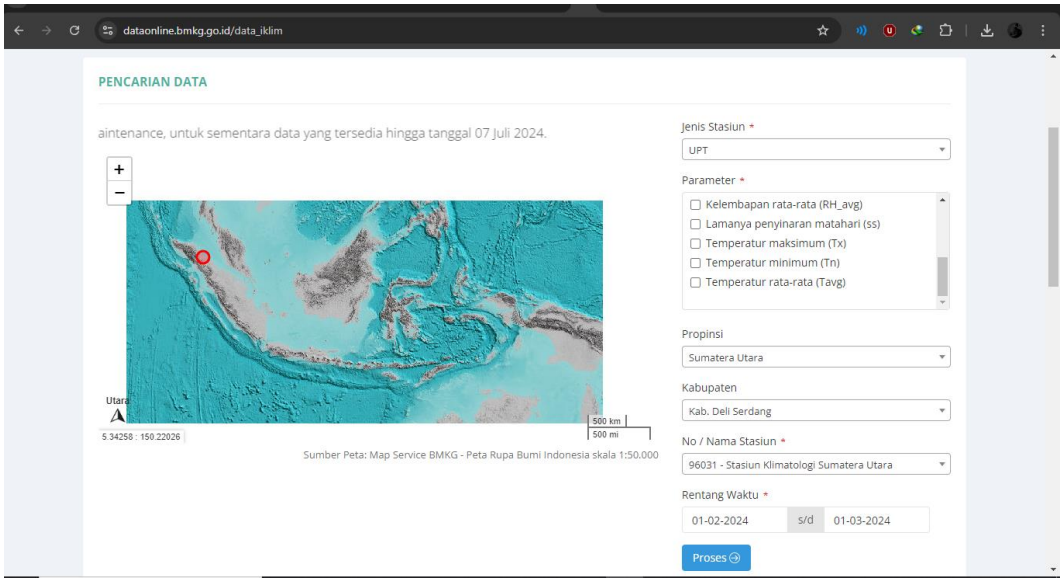
Gambar 4.5 Registrasi Akun

Sebelum bisa mengakses data, pengguna harus melakukan registrasi dan verifikasi akun pribadi pada halaman https://dataonline.bmkg.go.id/home, dihalaman tersebut juga tertera alur dan cara bagaimana mendaftarkan akun di website BMKG agar bias mengakses datanya secara gratis.



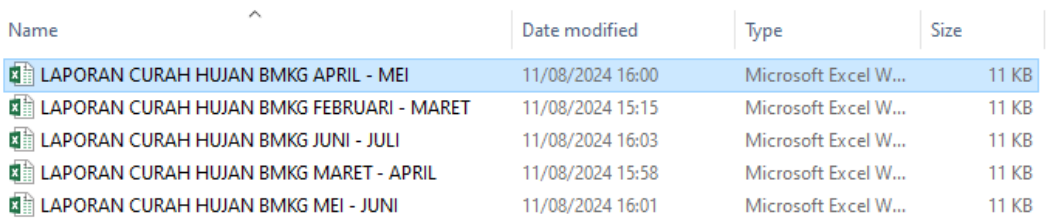
Gambar 4.6 Halaman Dashboard Website Data Online BMKG

Gambar diatas merupakan halaman dashboard pada data online, saat user berhasil registrasi akun, akan dilanjutkan ke web ini, bias dilihat user bias melihat informasi mengenai tanggal unduh data, jenis data yang diunduh, dan lainnya.



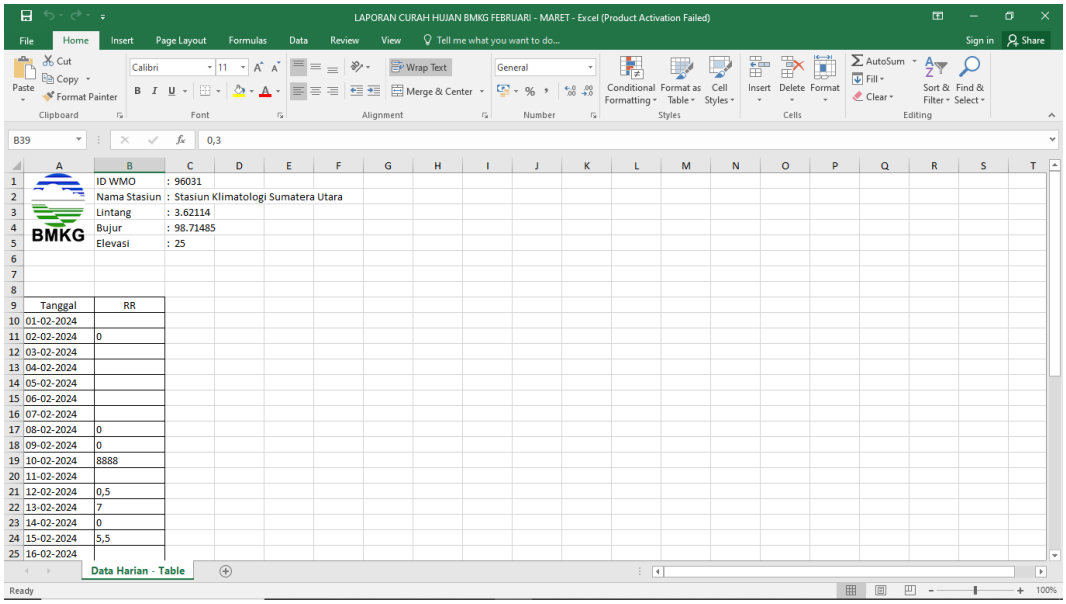
Gambar 4.7 Halaman Akses dan Download Data di website BMKG

Gambar diatas merupakan halaman untuk mengakses atau mendownload data yang diperlukan secara open source, bias dilihat pada sisi sebelah kanan, pengguna bisa memilih parameter, nama stasiun yang bertugas, provinsi, kabupaten, dan rentang waktu yang ingin diambil datanya. Perlu dicatat, data yang dapat diuntuh untuk rentang waktu sebulan saja.



Gambar 4.8 Sample Data Curah Hujan

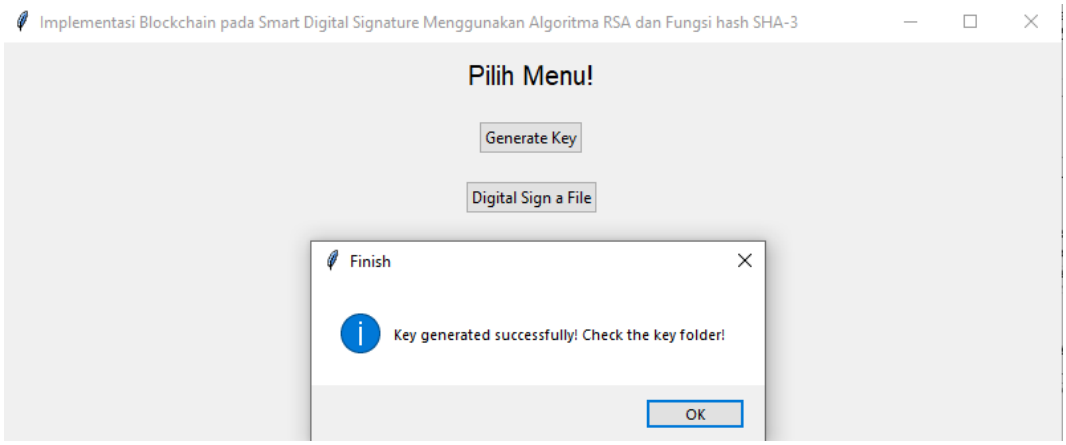
Data diatas merupakan sample data yang sudah diunduh untuk keperluan penelitian ini, data yang kemudian akan dienkripsi dan ditandatangani serta diverifikasi. Format file data adalah excel (.xlsl).



Gambar 4.9 Isi Dari Data Curah Hujan

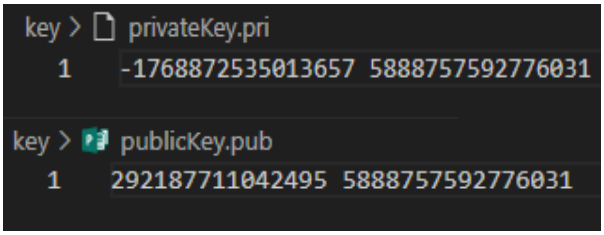
4.4 Implementasi Sistem dan Hasilnya

Langkah awal yang dilakukan yaitu menggenerate kunci public dan kunci private yang akan digunakan untuk nantinya untuk mengenkripsi dan mendeskripsi data/file yang ingin ditanda tangani dengan mengklik tombol “Generate Key”, kedua kunci tersebut bias dilihat di dalam key folder.



Gambar 4.10 Generate Kunci Public dan Private

Setelah kunci berhasil degenerate, maka kunci bisa diakses dan dilihat di dalam key folder, kunci tersebut bias dilihat pada gambar dibawah



Gambar 4.11 Kunci Public dan Kunci Private

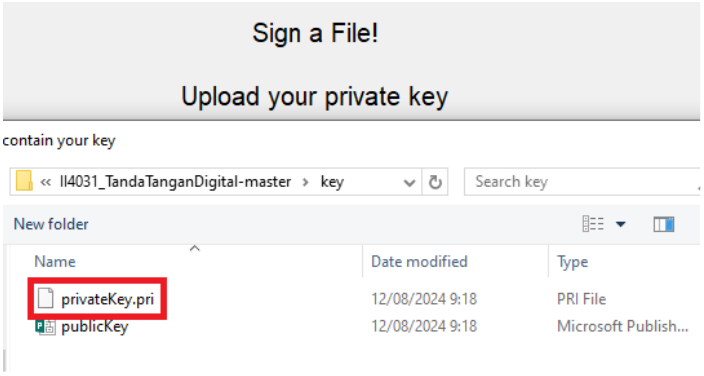
Langkah selanjutnya yaitu mengupload data/file yang ingin ditanda tangani, pada bagian Pilih Menu, klik tombol “Digital sign a File” untuk upload filenya

Gambar 4.12 Digital Sign a File

Kemudian sistem akan menghadapkan user untuk memilih file yang ingin ditanda tangani, bisa dilihat pada gambar dibawah, penulis memilih file sample dengan nama file “Laporan Curah Hujan BMKG Februari – Maret” untuk ditan tangani.

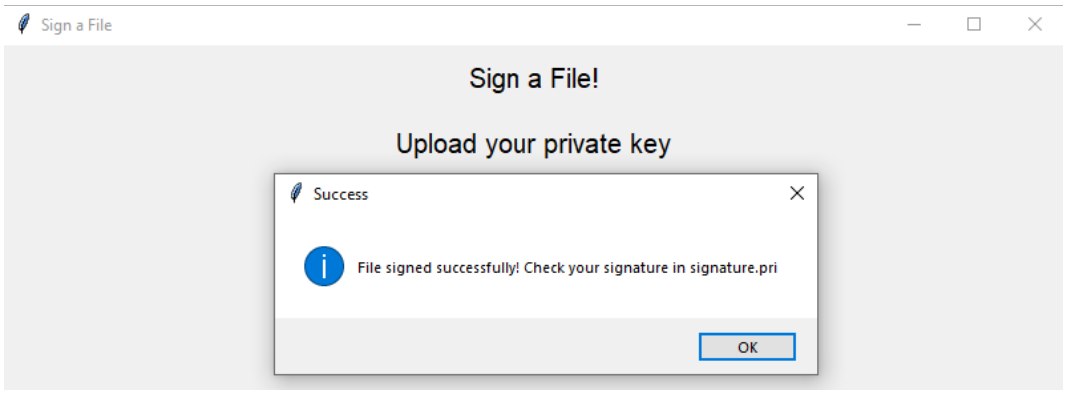
Gambar 4.13 Memilih File Untuk ditanda tangani

Setelah berhasil upload file, maka sistem memerintahkan untuk mengupload private key (kunci privat) untuk file tersebut ditanda tangani.

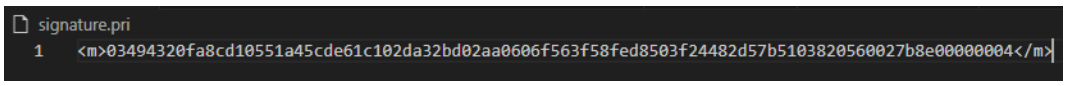


Gambar 4.14 Upload Private Key

Selanjutnya ketika file berhasil diupload, diberikan kunci private untuk ditanda tangani, kemudian hasilnya bias dilihat pada gambar dibawah, bahwa file sebelumnya yang diupload berhasil diberikan tanda tangan, hasilnya bisa di cek melalui file “signature.pri”.



Gambar 4.15 Success File Signed

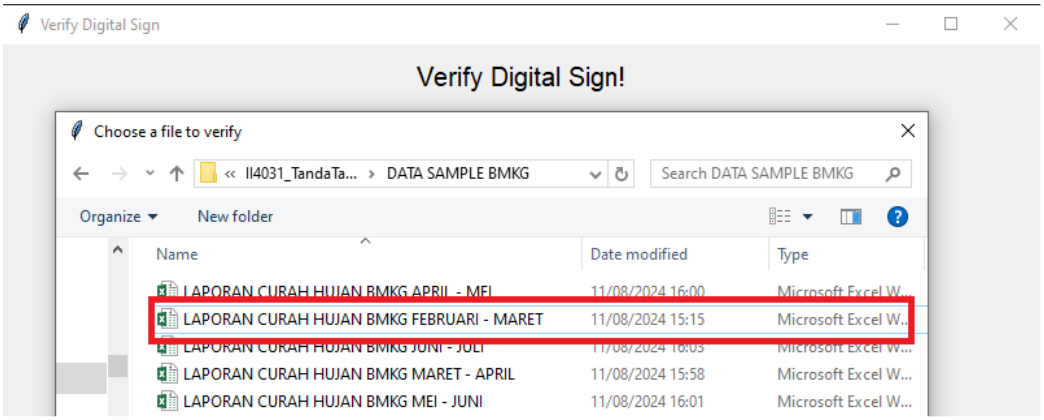


Gambar 4.16 Hasil File Yang Sudah Ditanda tangani

Kemudian setelah file berhasil ditanda tangani, file kemudian akan diverifikasi sebagai tanda bahwa sudah atau belum file tersebut diberikan tanda tangan sebelumnya, pada menu pilih bagian “Verify Digital Sugn”.

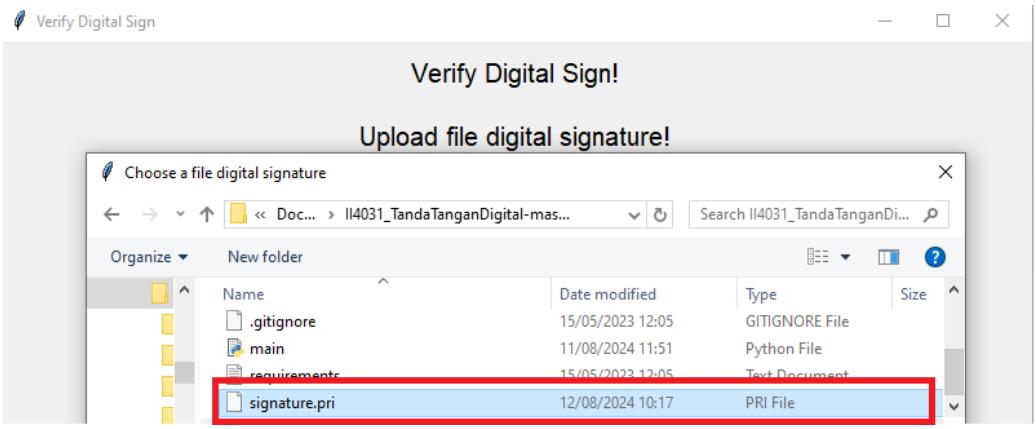
Gambar 4.17 Verify Digital Sign

Setelah klik tombol Verify, maka sistem memerintahkan untuk mengupluad file yang sudah ditanda tangani sebelumnya, upload file yang sudah ditanda tangi sebelumnya, disini file tersebut yaitu “Laporan Curah Hujan BMKG Februari – Maret”.



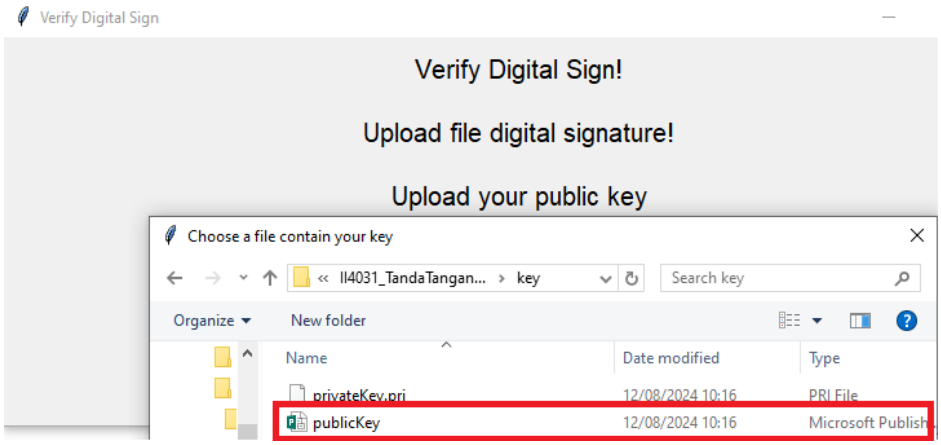
Gambar 4.18 Upload File Digital Signature Untuk Diverifikasi

Setelah file diupload, kemudian user harus upload file digital signature sebelumnya, file tersebut adalah file “signature.pri” yang digunakan untuk menanda tangani file yang sebelumnya yang sudah diberikan tanda tangan.



Gambar 4.19 Upload File Digital Signature

Kemudian Mengupload Public Key (Kunci Publik).



Gambar 4.20 Upload Kunci Publik

Jika semua kebutuhan file berhasil di upload, dan muncul notif seperti ini, berarti file sudah berhasil ditanda tangani dan juga sudah berhasil di verifikasi

Gambar 4.21 File Sukses Diverifikasi

Dengan demikian, file dengan nama “Laporan Curah Hujan BMKG Februari – Maret” sudah berhasil ditanda tangani dan diverifikasi.

Selanjutnya, hasil dari kelima file sample yang ditanda tangani hasilnya akan disajikan dalam tabel berikut:

Tabel 4.1 Hasil Uji Data Sampel Tanda Tangan Digital

No	Nama File	Digital Signature	Status Verifikasi	
			YA	TIDAK
1	Laporan Curah Hujan BMKG Februari – Maret (LAPORAN CURAH HUJAN BMKG FEBRUARI – MARET.xlsx)	03494320fa8cd10551a45cde61c102da32bd024 aa0606f563f58fed8503f24482d57b5103820560027b8e0000000	√	
2	Laporan Curah Hujan BMKG Maret – April (LAPORAN CURAH HUJAN BMKG MARET – APRIL.xlsx)	00858b79ce3546008eae7c94c6dc02555322bbcd 82028927f413815d01035790f73fa70410e17e82176b00000004	√	
3	Laporan Curah Hujan BMKG April – Mei (LAPORAN CURAH HUJAN BMKG APRIL – MEI.xlsx)	0a95ff7e56874d090cfbbe1f46440e8d44c583ce8 e088097a83d26d801d5c0492c3cee0909c0b1872d1400000004	√	
4	Laporan Curah Hujan BMKG Mei – Juni (LAPORAN CURAH HUJAN BMKG MEI – JUNI.xlsx)	1e58e5a1745722a27028806e0ce94eb82275020 a09d6f2c610ad06eb74d60a32ea1eb4e91d689e511fb000000003	√	
5	Laporan Curah Hujan BMKG Juni – Juli (LAPORAN CURAH HUJAN BMKG JUNI – JULI.xlsx)	05034be0c91b007700f7250306478e1aa2e90420c1649 2f5006f2eb326f700002192ff8f05b069f20b9300000003	√	

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan diskusi tentang penelitian yang telah penulis lakukan, beberapa hal berikut dapat disimpulkan:

1. Dengan penerapan blockchain pada smart digital signature, khususnya pada sample data curah hujan yang didapatkan secara online melalui website resmi lembaga BMKG, sekiranya bisa memberikan manfaat untuk mengamankan data data penting yang tidak disebarluaskan elalui online (close source).
2. Algoritma RSA dan SHA-3 dapat diterapkan kedalam blockchain pada smart digital signature untuk menandatangani data sample yang penulis dapat dari laman website BMKG langsung.
3. Perancangan sistem digital signature yang mengadopsi metode RSA dan SHA-3 dapat digunakan untuk menjaga data sehingga terhindar dari penyalahgunaan, serta memberikan verifikasi yang tepat untuk data data yang penting dan bersifat tertutup

5.2 Saran

Berdasarkan beberapa kesimpulan yang telah penulis jabarkan,, beberapa saran yang dapat diambil, antara lain:

1. Perlunya penambahan fitur yang lebih mendukung para peneliti seperti penlis, agar hasil yang didapatkan lebih maksimal, sekiranya lembaga lainnya bisa memiliki fitur seperti lembaga BMKG yang membuat fitur pengunduhan data secara open source, agar memudahkan banyak orang mendapatkan data secara praktis.
2. Sistem aplikasi yang penulis buat untuk pengembangan lebih lanjut, sehingga harus lebih banyak dievalusi, seperti penambahan fitur untuk convert data file nya ke format digital signature.
3. Algoritma RSA dan SHA-3 banyak digunakan dalam kriptografi, khususnya pada blockchain digital signature, perlunya perkembangan agar data selalu terjaga dengan adanya sistem yang lebih baik dan akurat, terutama sistem yang memiliki verifikasi yang kualitasnya lebih bagus.
4. Diharapkan bisa menambahkan extensi file lainnya yang lebih kompleks.

DAFTAR PUSTAKA

Ahram, T., et al. (2017). Blockchain technology innovations. *IEEE Technology & Engineering Management Conference (TEMSCON), 137-141*.

Allan, Joshua., et al. (2021). Implementasi Algoritma AES, ElGamal, dan SHA3 untuk Keamanan File Digital. *Jurnal Infra, 1-7.*

Alrido, Machsudirwan., et al. (2021). Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Data Nilai Siswa Pada SMK Multi Karya Medan. *Jurnal CyberTech Vol.4. No.3, Februari 2021 P-ISSN : 9800-3456 ρ 1 E-ISSN : 2675-9802*

Farhan, Faiz & Leman, Dedi. (2023). Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT. *Journal of Machine Learning and Data Analytics (MALDA) Volume 02, No. 01, Februari 2023 Page: 18-27 e-ISSN 2828-3465, 18-27.*

Fauzan, Dika Alfiani., et al. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web. *Journal of Information and Information Security (JIFORTY) Vol. 4, No. 1, Juni 2023, 91 – 104 e-ISSN : 2722-4058*

Khamsyar, Alif & Basri, Muh. (2022). Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) RSA. *JURNAL SINTAKS LOGIKA Vol.2 No.3 , September – 2022, 39-45*

Munir, Rinaldi. (2023). Algoritma RSA. Dapat diakeses pada *Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/10-Algoritma-RSA-2023.pdf*

Putri, I Gusti Ayu.,et al. (2022). Implementasi Kriptografi File Ujian Siswa Dengan Metode Rsa Berbasis Website Di Sman 84 Jakarta. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta – Indonesia, 06 September 2022, 130-139.*

Rakhmansyah, M., et al. (2021). Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT. *ADI Bisnis Digital Interdisiplin Jurnal, 2(1 Juni), 39-47.*

Sari, Morita. (2021). Analisis Algoritma SHA-3 Keamanan pada Data Pribadi. *Vol.5 No.2 April 2021 TECNOSCIENZA, 232-242.*

Sarumaha, Demonius., et al. (2024). Penerapan Algoritma Enhanced Dual Rivest Shamir Adleman untuk Pengamanan Data. *Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000 Volume 4, Number 1, Maret 2024, 34-41.*

Sugiarto., Muhammad & Purwanto, (2022). Implementasi Algoritma Rsa Untuk Perancangan Aplikasi Berbasis Java Desktop Pada Mts Daarul Falah. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta – Indonesia, 06 September 2022, 344-350*

Susanto, Ari Eko. (2023). Keamanan Pesan Teks Dengan Metode Enkripsi Dan Dekripsi Menggunakan Algoritma Rsa (Rivest Shamir Adleman) Berbasis Android. *Jurnal Teknologi Pintar Volume 3 (2), 2023, 1-16.*

Virgiawan,Muhammad Andhika & Utama, Gunawan Pria. (2020). Penggunaan Metode Ong-Schnorr-Shamir Pada Pembuatan Tanda Tangan Digital. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST), Volume05 Nomor 01, Juni 2020, ISSN: 2548-1916, e-ISSN: 2657-1501, 51-59.*

Waruwu., Erwin Vasi, *et al*. (2021). Penerapan Digital Signature Menggunakan Metode RSA Untuk Menvalidasi Keaslian Ijazah SMA Swasta Bina Artha. *Jurnal CyberTech Vol. 1, No. 1, September 2021 : pp. 37-47 P-ISSN : 1978-6603 E-ISSN: 2615-3475*

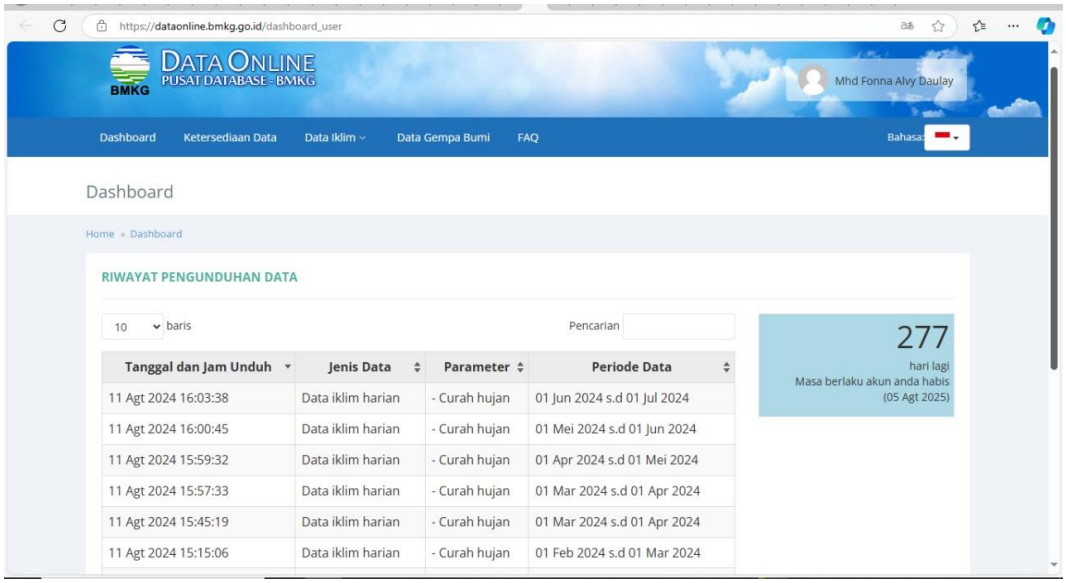
Widatama, Krisna., et al. (2022). Penggunaan Digital Signature Untuk Absensi Pada Universitas Muhammadiyah Purworejo. *Jurnal Sistem Cerdas (2022) Vol 05 - No 01 eISSN : 2622-8254, 36 – 45.*

Yusmaifany., et al. (2024). Aplikasi Enkripsi Data Video Menggunakan Metode Rsa Dan Blowfish Berbasis Web. *Jurnal Komputer Teknologi Informasi Sistem Komputer JUKTISI e-ISSN : 2963-7104 (Online) p-ISSN : 2962 3022 (Print) Volume 2 No 3 Februari 2024 - Page: 535-544*

Yusup, Muhamad., et al. (2019). Pemanfaatan Teknologi Blockchain Pada Program Sertifikasi Dosen. *Seminar Nasional Sistem Informasi dan Teknologi Informatika SENSITif 2019, 365-371.*

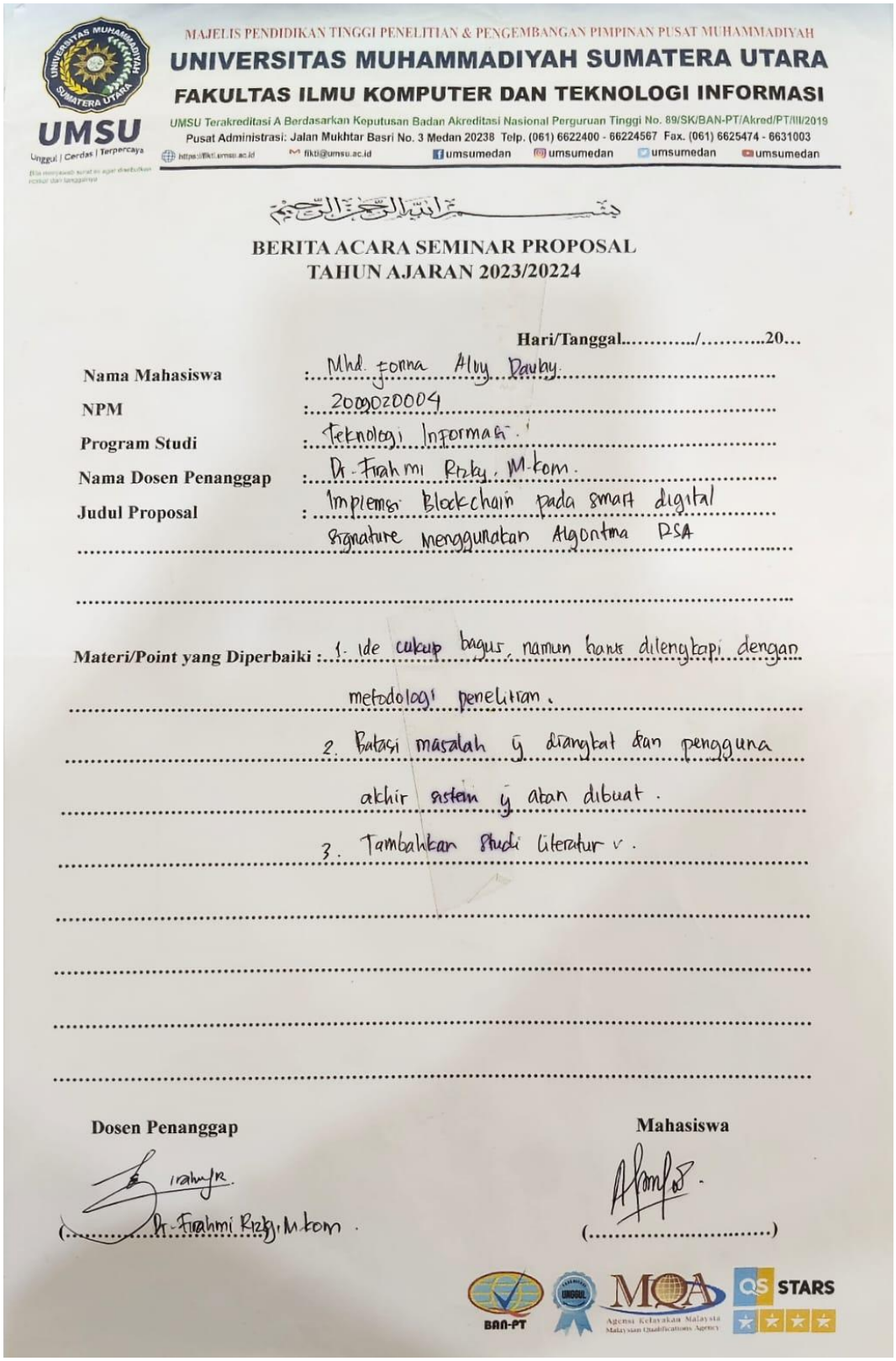
LAMPIRAN

1. Proses Pengunduhan Data Secara Online (Open Source) Melalui Website Resmi BMKG.



Tanggal dan Jam Unduh	Jenis Data	Parameter	Periode Data
11 Agt 2024 16:03:38	Data iklim harian	- Curah hujan	01 Jun 2024 s.d 01 Jul 2024
11 Agt 2024 16:00:45	Data iklim harian	- Curah hujan	01 Mei 2024 s.d 01 Jun 2024
11 Agt 2024 15:59:32	Data iklim harian	- Curah hujan	01 Apr 2024 s.d 01 Mei 2024
11 Agt 2024 15:57:33	Data iklim harian	- Curah hujan	01 Mar 2024 s.d 01 Apr 2024
11 Agt 2024 15:45:19	Data iklim harian	- Curah hujan	01 Mar 2024 s.d 01 Apr 2024
11 Agt 2024 15:15:06	Data iklim harian	- Curah hujan	01 Feb 2024 s.d 01 Mar 2024

2. Berita Acara Seminar Proposal oleh Dosen Penguji



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

UMSU
Unggul | Cerdas | Terpercaya

بسم الله الرحمن الرحيم

BERITA ACARA SEMINAR PROPOSAL
TAHUN AJARAN 2023/20224

Hari/Tanggal...../.....20...

Nama Mahasiswa : Muhd. Jorma Alvy Daulay
NPM : 2009020004
Program Studi : Teknologi Informasi
Nama Dosen Penanggap : Dr. Fahmi Rizky, M.kom.
Judul Proposal : Implemsi Blockchain pada smart digital signature menggunakan Algoritma RSA

Materi/Point yang Diperbaiki :
1. Ide cukup bagus, namun harus dilengkapi dengan metodologi penelitian.
2. Batasi masalah yg diangkat dan pengguna akhir sistem yg akan dibuat.
3. Tambahkan studi literatur v.

Dosen Penanggap

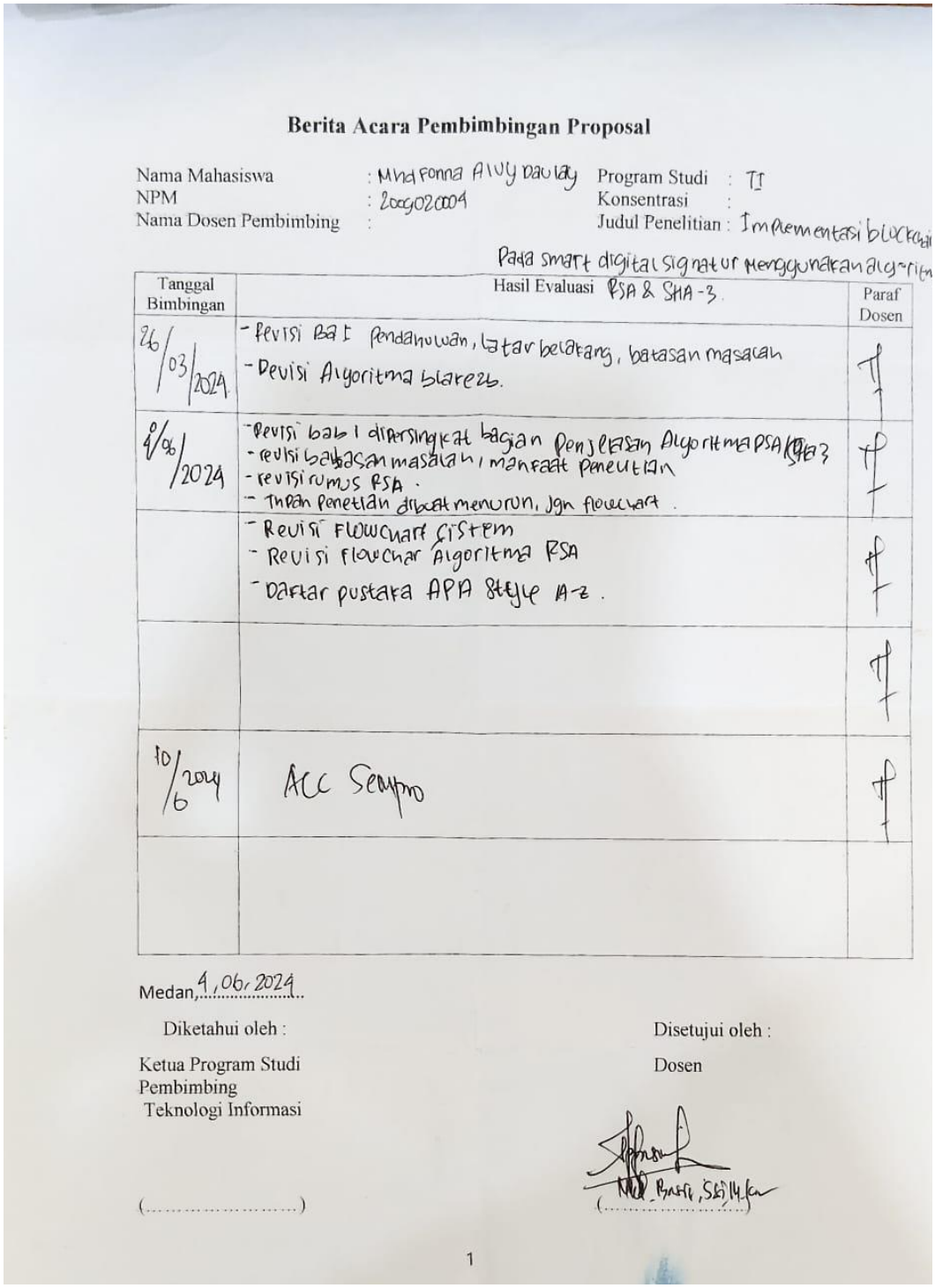
Dr. Fahmi Rizky, M.kom.

Mahasiswa

(.....)

BAN-PT MQA Agensi Kelayakan Malaysia Malaysian Qualifications Agency QS STARS

3. Berita Acara Bimbingan Proposal Skripsi (Seminar Proposal).



Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Mhd Fonna Alvy Daulay
NPM : 2009020004
Nama Dosen Pembimbing :
Program Studi : TI
Konsentrasi :
Judul Penelitian : Implementasi blockch
Pada smart digital signatur menggunakan algorit

Tanggal Bimbingan	Hasil Evaluasi RSA & SHA-3.	Paraf Dosen
26/03/2024	- Revisi BAB I pendahuluan, latar belakang, batasan masalah - Revisi Algoritma blake2b.	
4/06/2024	- Revisi bab I diarsingkat bagian penjelasan Algoritma RSA & SHA3 - revisi batasan masalah, manfaat penelitian - revisi rumus RSA. - Tujuan penelitian dibuat menurun, jgn flowchart.	
	- Revisi Flowchart sistem - Revisi flowchar Algoritma RSA - Daftar pustaka APA style A-Z.	
10/6/2024	ACC Sempro	

Medan, 4 Juni 2024

Diketahui oleh :
Ketua Program Studi
Pembimbing
Teknologi Informasi

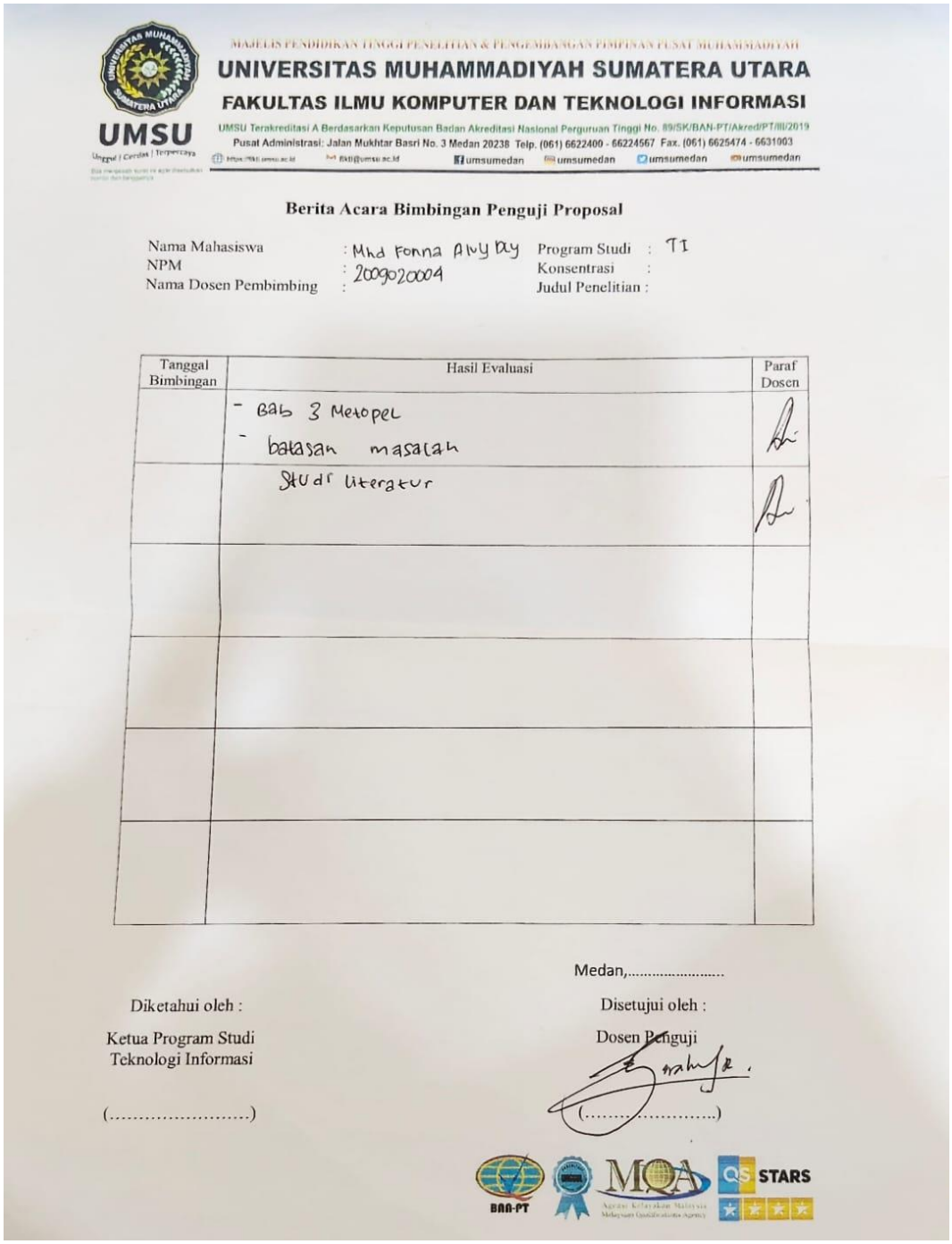
(.....)

Disetujui oleh :
Dosen

(.....)

1

4. Berita Acara Proposal Skripsi Oleh Dosen Penguji (Setelah Sempro).



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

umsumedan umsumedan umsumedan umsumedan

Berita Acara Bimbingan Penguji Proposal

Nama Mahasiswa : Mhd Fonna Alwy Dy
NPM : 2009020004
Nama Dosen Pembimbing :

Program Studi : TI
Konsentrasi :
Judul Penelitian :

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
	- Bab 3 Metopel - batasan masalah	
	Studi literatur	

Medan,.....

Diketahui oleh :

Ketua Program Studi
Teknologi Informasi

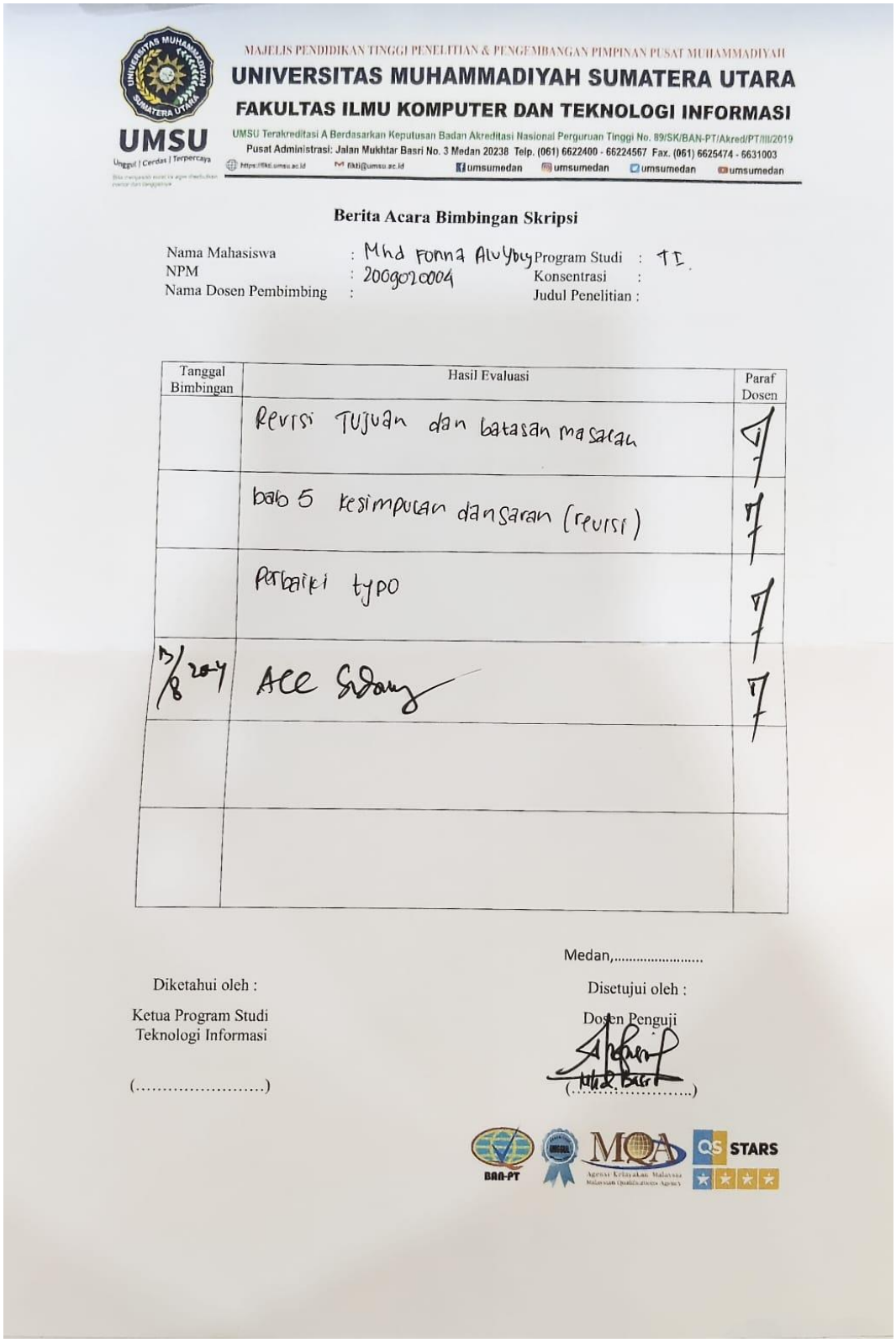
(.....)

Disetujui oleh :

Dosen Penguji

(.....)

5. Berita Acara Bimbingan Skripsi (Sidang).



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Berita Acara Bimbingan Skripsi

Nama Mahasiswa : Mhd Fonna Alvyby
NPM : 2009020004
Nama Dosen Pembimbing :
Program Studi : TI
Konsentrasi :
Judul Penelitian :

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
	Revisi Tujuan dan batasan masalah	
	bab 5 kesimpulan dan saran (revisi)	
	perbaiki typo	
13/8 2024	Acc Sidang	

Medan,.....

Diketahui oleh :
Ketua Program Studi
Teknologi Informasi

(.....)

Disetujui oleh :
Dosen Penguji

(.....)

BAN-PT