

**RANCANG BANGUN SISTEM E-VOTING HIMPUNAN MAHASISWA
MENGUNAKAN ALGORITMA PAILLIER PADA UNIVERSITAS
MULTIMEDIA NUSANTARA**



SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

Ivan Tenusa

00000026772

UMN

UNIVERSITAS

MULTIMEDIA

NUSANTARA

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2022

**RANCANG BANGUN SISTEM E-VOTING HIMPUNAN MAHASISWA
MENGUNAKAN ALGORITMA PAILLIER PADA UNIVERSITAS
MULTIMEDIA NUSANTARA**



SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

Ivan Tenusa
0000026772

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2022

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Ivan Tenusa
Nomor Induk Mahasiswa : 00000026772
Program Studi : Informatika

Skripsi dengan judul:

Rancang Bangun Sistem E-Voting Himpunan Mahasiswa Menggunakan Algoritma Paillier pada Universitas Multimedia Nusantara

merupakan hasil karya saya sendiri bukan plagiat dari karya ilmiah yang ditulis oleh orang lain, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/ penyimpangan, baik dalam pelaksanaan Skripsi maupun dalam penulisan laporan Skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk Tugas akhir yang telah saya tempuh.

UMM

Tangerang, 17 Juni 2022



UNIVERSITAS
MULTIMEDIA
NUSANTARA

(Ivan Tenusa)

HALAMAN PENGESAHAN

Skripsi dengan judul

RANCANG BANGUN SISTEM E-VOTING HIMPUNAN MAHASISWA MENGUNAKAN ALGORITMA PAILLIER PADA UNIVERSITAS MULTIMEDIA NUSANTARA

oleh

Nama : Ivan Tenusa
NIM : 00000026772
Program Studi : Informatika
Fakultas : Fakultas Teknik dan Informatika

Telah diujikan pada hari Jumat, 1 Juli 2022

Pukul 13.00 s/d 15.00 dan dinyatakan

LULUS

Dengan susunan penguji sebagai berikut

Ketua Sidang

Penguji

(Alexander Waworuntu, S.Kom., M.T.I.)

NIDN: 0309068503

Pembimbing I

(Vincentius Kurniawan, S.Kom.,

M.Eng.Sc)

NIDN: 0308079501

Pembimbing II

(Eunike Endariahna Surbakti, S.Kom., M.T.I.) (Fenina Adline Twince Tobing, S.Kom., M.Kom.)

NIDN: 0322099401

NIDN: 0406058802

Ketua Program Studi Informatika,

(Marlinda Vasty Overbeek, S.Kom., M.Kom.)

NIDN: 0818038501

**HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Ivan Tenusa
NIM : 00000026772
Program Studi : Informatika
Fakultas : Teknik dan Informatika
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

**RANCANG BANGUN SISTEM E-VOTING HIMPUNAN MAHASISWA
MENGUNAKAN ALGORITMA PAILLIER PADA UNIVERSITAS
MULTIMEDIA NUSANTARA**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non eksklusif ini Universitas Multimedia Nusantara berhak menyimpan, mengalih media / format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis / pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

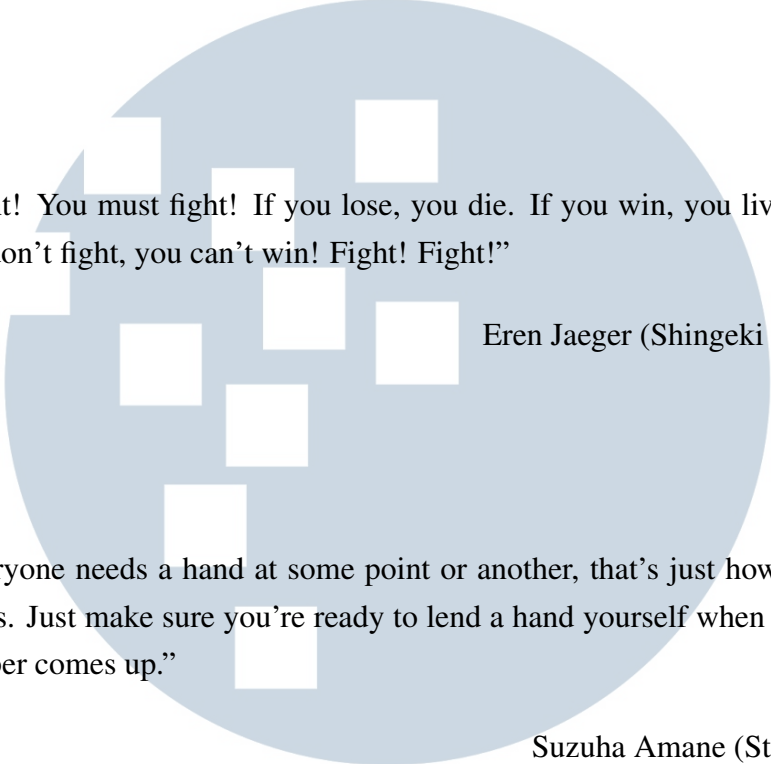
Tangerang, 17 Juni 2022
Yang menyatakan

UNIVERSITA
MULTIMEDIA
NUSANTARA



Ivan Tenusa

Halaman Persembahan / Motto



”Fight! You must fight! If you lose, you die. If you win, you live. If you don’t fight, you can’t win! Fight! Fight!”

Eren Jaeger (Shingeki no Kyojin)

”Everyone needs a hand at some point or another, that’s just how life works. Just make sure you’re ready to lend a hand yourself when your number comes up.”

Suzuha Amane (Steins;Gate)

UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Skripsi ini dengan judul Rancang Bangun Sistem E-Voting Himpunan Mahasiswa Menggunakan Algoritma Paillier pada Universitas Multimedia Nusantara yang dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Jurusan Informatika Pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Ibu Marlinda Vasty Overbeek, S.Kom., M.Kom., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Ibu Eunike Endariahna Surbakti, S.Kom., M.T.I., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi sehingga skripsi ini dapat selesai.
5. Ibu Fenina Adline Twince Tobing, S.Kom., M.Kom., sebagai Pembimbing kedua yang telah banyak membantu dan memberikan bimbingan sehingga skripsi ini dapat selesai.
6. Orang Tua, keluarga, dan teman-teman yang telah memberikan bantuan dukungan sehingga skripsi ini dapat selesai.

Semoga skripsi ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi bagi para pembaca.

Tangerang, 17 Juni 2022



Ivan Tenusa

RANCANG BANGUN SISTEM E-VOTING HIMPUNAN MAHASISWA MENGUNAKAN ALGORITMA PAILLIER PADA UNIVERSITAS MULTIMEDIA NUSANTARA

Ivan Tenusa

ABSTRAK

Organisator himpunan mahasiswa di Universitas Multimedia Nusantara bertugas bertugas untuk memberdayakan, memfasilitasi, dan membantu perkembangan mahasiswa, dosen, dan alumni program studi himpunan tersebut. Bila wakil yang terpilih tidak mewakili suara mahasiswa yang diwakili, maka permasalahan akan mudah muncul. Oleh karena itu, tingkat partisipasi mahasiswa dalam proses pemungutan suara sangatlah penting. Jika tingkat partisipasi mahasiswa rendah, maka risiko suara mayoritas tidak terdengar akan meningkat. Data dari KPU UMN menunjukkan bahwa partisipasi mahasiswa Fakultas Teknik dan Informatika dalam pemilu 2021 masih sangat kurang, dengan 3 dari 4 fakultas memiliki tingkat partisipasi kurang dari 50%. Penelitian ini membangun sebuah sistem pemungutan suara untuk Himpunan Mahasiswa Universitas Multimedia Nusantara untuk menggantikan sistem Google Form yang sebelumnya digunakan dan diharapkan dapat meningkatkan tingkat partisipasi mahasiswa dalam pemilu di masa depan. Algoritma enkripsi homomorfis Paillier digunakan dalam sistem yang dibangun untuk melakukan enkripsi dan dekripsi data suara yang diberikan oleh pemberi suara agar suara tersebut dapat terjamin kerahasiaannya. Algoritma tersebut dipilih karena relatif baru, lebih cepat dibandingkan algoritma enkripsi homomorfis lainnya, dan relevan untuk implementasi dalam penelitian ini. Uji coba pengguna pada aplikasi yang telah dibangun dengan menggunakan *Technology Acceptance Model (TAM)* menunjukkan bahwa aplikasi yang telah dibuat dapat dinyatakan berhasil dengan hasil penilaian pengguna sebesar 87,50% pada kategori *perceived ease-of-use*, 72,27% pada kategori *perceived usefulness*, 74,74% pada kategori *behavioral intention*, dan 86,46% pada kategori *actual usage*.

Kata kunci: *E-Voting*, himpunan mahasiswa, *Paillier*, sistem voting, Universitas Multimedia Nusantara

UNIVERSITAS
MULTIMEDIA
NUSANTARA

Designing and Building a Student Association E-Voting System in Universitas Multimedia Nusantara Using Paillier Algorithm

Ivan Tenusa

ABSTRACT

The student association representatives in Universitas Multimedia Nusantara are tasked to empower, facilitate, and foster the growth of the students, lecturers, and alumni of their respective program. If the elected representatives does not align with the general consensus, then problems will inevitably arise. As such, student participation in the yearly voting period is paramount. When the voting participation is low, the risk of majority voice to not be heard will increase. Data from KPU UMN shows that among the 4 student association in Tech and IT Faculty in Universitas Multimedia Nusantara, 3 of them have a participation rate lower than 50%. This research aims to build an E-Voting system for Student Associations in Universitas Multimedia Nusantara so that it will be able to replace the currently used Google Form system and hopefully result in an increase in student participation for future voting periods. Paillier homomorphic encryption algorithm is used in the system to encrypt and decrypt voting messages sent by voters to ensure its secrecy. The algorithm was chosen for its relative recency, speed, and relevancy to this research compared to other algorithms. User acceptance test using Technology Acceptance Model (TAM) has shown that the application has been successfully built with user assessment of 87,50% for perceived ease-of-use, 72,27% for perceived usefulness, 74,74% for behavioral intention, and 86,46% for actual usage.

Keywords: *E-Voting, Paillier, student association, Universitas Multimedia Nusantara, voting system*

U M N
U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

DAFTAR ISI

| | |
|--|------|
| HALAMAN JUDUL | i |
| PERNYATAAN TIDAK MELAKUKAN PLAGIAT | ii |
| HALAMAN PENGESAHAN | iii |
| HALAMAN PERSETUJUAN PUBLIKASI ILMIAH | iv |
| HALAMAN PERSEMBAHAN/MOTO | v |
| KATA PENGANTAR | vi |
| ABSTRAK | vii |
| ABSTRACT | viii |
| DAFTAR ISI | ix |
| DAFTAR GAMBAR | x |
| DAFTAR TABEL | xii |
| DAFTAR LAMPIRAN | xiii |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang Masalah | 1 |
| 1.2 Rumusan Masalah | 4 |
| 1.3 Batasan Permasalahan | 4 |
| 1.4 Tujuan Penelitian | 5 |
| 1.5 Manfaat Penelitian | 5 |
| 1.6 Sistematika Penulisan | 6 |
| BAB 2 LANDASAN TEORI | 7 |
| 2.1 Rancang Bangun Sistem E-Voting | 7 |
| 2.2 Algoritma Enkripsi Paillier | 9 |
| 2.3 Arsitektur Framework Model-View-Controller | 11 |
| 2.4 Pemilihan Umum Himpunan Mahasiswa di UMN | 12 |
| BAB 3 METODOLOGI PENELITIAN | 14 |
| 3.1 Metodologi Penelitian | 14 |
| 3.2 Perumusan Kebutuhan Sistem | 16 |
| 3.2.1 Use Case Diagram | 16 |
| 3.2.2 Entity Relationship Diagram | 17 |
| 3.3 Perancangan Sistem | 19 |
| 3.3.1 Data Flow Diagram | 19 |
| 3.3.2 Database Schema | 21 |
| 3.3.3 Flowchart | 27 |
| 3.4 Mockup Sistem | 43 |
| BAB 4 HASIL DAN DISKUSI | 54 |
| 4.1 Spesifikasi Sistem | 54 |
| 4.2 Implementasi | 54 |
| 4.2.1 Tampilan Halaman | 54 |
| 4.2.2 Implementasi Algoritma Paillier | 67 |
| 4.3 Uji Coba Algoritma Paillier | 72 |
| 4.4 Uji Penerimaan Pengguna | 76 |
| BAB 5 SIMPULAN DAN SARAN | 81 |
| 5.1 Simpulan | 81 |
| 5.2 Saran | 81 |
| DAFTAR PUSTAKA | 82 |

DAFTAR GAMBAR

| | | |
|-------------|--|----|
| Gambar 2.1 | Proposal model sistem voting elektronik oleh Chauhan . . . | 8 |
| Gambar 3.1 | <i>Use Case Diagram</i> | 16 |
| Gambar 3.2 | <i>Entity Relationship Diagram</i> | 18 |
| Gambar 3.3 | <i>Data Flow Diagram Level 0</i> | 19 |
| Gambar 3.4 | <i>Data Flow Diagram Level 1</i> | 20 |
| Gambar 3.5 | <i>Database Schema</i> | 22 |
| Gambar 3.6 | Flowchart Utama | 28 |
| Gambar 3.7 | Flowchart Halaman Awal | 29 |
| Gambar 3.8 | Flowchart Navigasi Halaman Pengunjung | 30 |
| Gambar 3.9 | Flowchart Pengecekan Halaman Pemberian Suara | 32 |
| Gambar 3.10 | Flowchart Login | 33 |
| Gambar 3.11 | Flowchart Pemberian Suara | 35 |
| Gambar 3.12 | Flowchart Enkripsi Data Suara | 36 |
| Gambar 3.13 | Flowchart Dekripsi Data Suara | 37 |
| Gambar 3.14 | Flowchart Pengiriman Kontak | 38 |
| Gambar 3.15 | Flowchart Navigasi Halaman Administrator | 39 |
| Gambar 3.16 | Flowchart Manajemen Data Oleh Admin | 41 |
| Gambar 3.17 | Flowchart Logout | 42 |
| Gambar 3.18 | Mockup Halaman Awal | 43 |
| Gambar 3.19 | Mockup Halaman Beranda | 44 |
| Gambar 3.20 | Mockup Halaman Login | 45 |
| Gambar 3.21 | Mockup Halaman Pemberian Suara | 46 |
| Gambar 3.22 | Mockup Konfirmasi Pemberian Suara | 46 |
| Gambar 3.23 | Mockup Umpan Balik Pemberian Suara | 47 |
| Gambar 3.24 | Mockup Notifikasi Sudah Memberikan Suara | 48 |
| Gambar 3.25 | Mockup Halaman Hasil Pemilu | 49 |
| Gambar 3.26 | Mockup Halaman Kontak | 50 |
| Gambar 3.27 | Mockup Notifikasi Pengiriman Pesan | 51 |
| Gambar 3.28 | Mockup Header Dropdown Administrator | 52 |
| Gambar 3.29 | Mockup Tabel Halaman Admin | 52 |
| Gambar 4.1 | Tampilan Halaman Awal | 55 |
| Gambar 4.2 | Tampilan Halaman Beranda | 56 |
| Gambar 4.3 | Tampilan Halaman Login | 56 |
| Gambar 4.4 | Tampilan Halaman Pemberian Suara | 57 |
| Gambar 4.5 | Tampilan Konfirmasi Pemberian Suara | 58 |
| Gambar 4.6 | Tampilan Notifikasi Keberhasilan Pemberian Suara | 58 |
| Gambar 4.7 | Tampilan Notifikasi Telah Memberikan Suara | 59 |
| Gambar 4.8 | Tampilan Halaman Hasil Pemilu | 59 |
| Gambar 4.9 | Tampilan Notifikasi Pemilu Belum Selesai | 60 |
| Gambar 4.10 | Tampilan Halaman Kontak | 61 |
| Gambar 4.11 | Tampilan Tabel Administrator | 61 |
| Gambar 4.12 | Tampilan Pemasukan Data oleh Administrator | 62 |
| Gambar 4.13 | Tampilan Pembaruan Data oleh Administrator | 63 |
| Gambar 4.14 | Tampilan Penghapusan Data oleh Administrator | 63 |
| Gambar 4.15 | Tampilan Halaman Awal di Layar Kecil | 64 |
| Gambar 4.16 | Tampilan Header di Layar Kecil | 65 |
| Gambar 4.17 | Tampilan Halaman Beranda di Layar Kecil | 65 |
| Gambar 4.18 | Tampilan Halaman Pemberian Suara di Layar Kecil | 66 |

| | | |
|-------------|--|----|
| Gambar 4.19 | Tampilan Halaman Hasil Pemilu di Layar Kecil | 67 |
| Gambar 4.20 | Gambar Potongan Kode Verifikasi Suara | 68 |
| Gambar 4.21 | Gambar Potongan Kode Enkripsi Suara | 69 |
| Gambar 4.22 | Gambar Potongan Kode Penyimpanan Suara | 70 |
| Gambar 4.23 | Gambar Potongan Kode Pengecekan Akun | 70 |
| Gambar 4.24 | Gambar Potongan Kode Fungsi Utama Dekripsi | 71 |
| Gambar 4.25 | Gambar Potongan Kode Fungsi Penjumlahan Suara | 71 |
| Gambar 4.26 | Gambar Potongan Kode Dekripsi Total Suara | 72 |
| Gambar 4.27 | Gambar Potongan Kode Menampilkan Hasil Pemilu | 72 |
| Gambar 4.28 | Daftar Hasil Enkripsi Suara Uji Coba Untuk ACES | 73 |
| Gambar 4.29 | Hasil Pemilu Uji Coba Untuk ACES | 73 |
| Gambar 4.30 | Daftar Hasil Enkripsi Suara Uji Coba Untuk HIMFERA | 74 |
| Gambar 4.31 | Hasil Pemilu Uji Coba Untuk HIMFERA | 75 |



DAFTAR TABEL

| | | |
|------------|---|----|
| Tabel 3.1 | Struktur Tabel Mahasiswa | 23 |
| Tabel 3.2 | Struktur Tabel Pasangan Calon | 24 |
| Tabel 3.3 | Struktur Tabel Himpunan | 25 |
| Tabel 3.4 | Struktur Tabel Voting Ballot | 25 |
| Tabel 3.5 | Struktur Tabel Kontak Pengguna | 26 |
| Tabel 3.6 | Struktur Tabel Kutipan Halaman Awal | 26 |
| Tabel 3.7 | Struktur Tabel Latar Belakang | 27 |
| Tabel 4.1 | Tabel Numerifikasi Data Suara Untuk Jumlah Maksimal Pemberi Suara 9999 | 68 |
| Tabel 4.2 | Tabel Dekripsi Manual Suara Uji Coba Individual untuk ACES | 74 |
| Tabel 4.3 | Tabel Dekripsi Manual Suara Uji Coba Individual untuk HIMFERA | 75 |
| Tabel 4.4 | Daftar Pertanyaan | 76 |
| Tabel 4.5 | Hasil Kuesioner | 77 |
| Tabel 4.6 | Rekapitulasi Evaluasi <i>Perceived Ease-of-Use</i> | 78 |
| Tabel 4.7 | Rekapitulasi Evaluasi <i>Perceived Usefulness</i> | 79 |
| Tabel 4.8 | Rekapitulasi Evaluasi <i>Behavioral Intention</i> | 79 |
| Tabel 4.9 | Rekapitulasi Evaluasi <i>Actual Usage</i> | 80 |
| Tabel 4.10 | Rekapitulasi Akhir Tingkat Penerimaan Pengguna Terhadap Aplikasi | 80 |



DAFTAR LAMPIRAN

| | |
|---|----|
| Lampiran 1. <i>Curriculum Vitae</i> | 84 |
| Lampiran 2. Transkrip Wawancara dengan Ketua HIMSI UMN | 86 |
| Lampiran 3. Transkrip Wawancara dengan mahasiswa UMN | 88 |
| Lampiran 4. Hasil Kuesioner | 89 |
| Lampiran 5. Hasil Pemungutan Suara dari Uji Coba Pengguna | 92 |
| Lampiran 6. Form Bimbingan dengan Dosen Pembimbing 1 | 94 |
| Lampiran 7. Form Bimbingan dengan Dosen Pembimbing 2 | 96 |
| Lampiran 8. Hasil Pengecekan Turnitin | 97 |

