

## Aplikasi Keamanan *E-Voting* Pemilihan Ketua Osis Menggunakan Metode AES 128 Berbasis Android (Studi Kasus: MTSN 3 Poso)

Shibghotullah Al Murod<sup>1</sup>, Suhirman<sup>1</sup>

<sup>1</sup>Program Studi Informatika, Universitas Teknologi Yogyakarta, Indonesia.

---

### Artikel Info

#### Kata Kunci:

AES-128;  
Enkripsi;  
*E-voting*;  
Keamanan Data;  
Kriptografi.

#### Keywords:

AES-128;  
Encryption;  
*E-voting*;  
Data Security;  
Cryptography.

---

### Riwayat Artikel:

Submitted: 16 Oktober 2024  
Accepted: 30 November 2024  
Published: 30 November 2024

**Abstrak:** Indonesia merupakan negara demokrasi yang rutin melaksanakan pemilu, termasuk dalam lingkup organisasi kecil seperti pemilihan ketua OSIS. Namun, metode pemilihan konvensional sering kali menghadapi berbagai masalah, seperti risiko kecurangan, kerahasiaan data yang rendah, dan proses penghitungan yang memakan waktu. Seiring perkembangan teknologi, *e-voting* menjadi alternatif yang menawarkan efisiensi dan transparansi. Meski demikian, aspek keamanan data menjadi tantangan utama dalam penerapan *e-voting*, mengingat data suara yang bersifat rahasia harus terlindungi dari ancaman manipulasi atau kebocoran informasi. Penelitian ini mengusulkan solusi dengan mengembangkan aplikasi *e-voting* berbasis Android menggunakan algoritma Advanced Encryption Standard (AES) 128-bit. Algoritma ini dipilih karena keandalannya dalam mengamankan data melalui proses enkripsi yang efisien, sehingga memastikan kerahasiaan suara, integritas data, dan keaslian pengguna. Data yang digunakan meliputi data pemilih, data suara, dan hasil perhitungan, yang dienkripsi sebelum disimpan atau diproses. Hasil penelitian menunjukkan bahwa aplikasi ini berhasil meningkatkan keamanan data pemilihan ketua OSIS di MTsN 3 Poso, serta memberikan efisiensi yang signifikan dibandingkan metode pemilihan konvensional. Dengan algoritma AES-128, data penting terjamin keamanannya selama proses pemilihan berlangsung. Aplikasi ini diharapkan menjadi solusi inovatif untuk menciptakan sistem pemilu yang lebih modern, aman, dan terpercaya.

**Abstract:** Indonesia is a democratic country that routinely holds elections, including in small organizations such as the election of the OSIS chairman. However, conventional election methods often face various problems, such as the risk of fraud, low data confidentiality, and time-consuming counting processes. Along with the development of technology, *e-voting* has become an alternative that offers efficiency and transparency. However, the aspect of data security is a major challenge in the implementation of *e-voting*, considering that confidential voting data must be protected from the threat of manipulation or information leakage. This study proposes a solution by developing an Android-based *e-voting* application using the Advanced Encryption Standard (AES) 128-bit algorithm. This algorithm was chosen because of its reliability in securing data through an efficient encryption process, thus ensuring vote confidentiality, data integrity, and user authenticity. The data used includes voter data, vote data, and calculation results, which are encrypted before being stored or processed. The results of the study show that this application has succeeded in increasing the security of OSIS chairman election data at MTsN 3 Poso, as well as providing significant efficiency compared to conventional election methods. With the AES-128 algorithm, important data is guaranteed to be secure during the election process. This application is expected to be an innovative solution to create a more modern, safe and reliable election system.

**Corresponding Author:**

Shibghotullah Al Murod

Email: shibghotullah.5210411087@student.uty.ac.id

---

**PENDAHULUAN**

Indonesia merupakan negara dengan penduduk terbanyak ke -4 di dunia dengan jumlah penduduk sebanyak 280,73 juta jiwa pada desember 2023 menurut data oleh katadata.co.id yang dilansir dari data kependudukan Direktorat Jendral Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri. Dengan jumlah jiwa sebanyak itu negara Indonesia menganut paham demokrasi, dan setiap 5 tahun sekali akan diadakan voting untuk memilih kepala negara yang akan memimpin untuk memimpin untuk 5 tahun mendatang.

Voting atau pemungutan suara itu sendiri secara sederhana dapat diartikan sebagai pilihan untuk memilih sebuah pilihan (Evans, 2004). Voting digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat, dan kemudian menemukan jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan (Arif, 2021). Para pemilih umumnya akan memilih kandidat yang mereka rasa mewakili pemikiran mereka atau kandidat yang mereka rasa akan memberi manfaat signifikan bagi para pemilih. Penggunaan voting paling sederhana dapat digunakan dalam ruang lingkup keluarga dan paling kompleks dalam ruang lingkup bernegara.

Seiring perkembangan zaman, manusia akan terdorong untuk menciptakan inovasi-inovasi baru. Salah satu inovasi tersebut adalah elektronik voting, pemilih akan menggunakan perangkat elektronik untuk memilih dan suara pemilih akan direkam secara digital. Tujuan dari electronic voting adalah menyelenggarakan pemungutan suara dengan biaya hemat dan penghitungan suara yang cepat dengan menggunakan sistem yang aman dan mudah untuk dilakukan audit (Risnanto, 2018)

Dalam era digital yang semakin berkembang, teknologi informasi menawarkan solusi untuk mengatasi berbagai permasalahan yang dihadapi dalam pemilihan tradisional. Salah satu solusi tersebut adalah penerapan sistem e-voting (electronic voting). E-voting adalah metode pemilihan yang memanfaatkan teknologi digital untuk memungkinkan pemilih memberikan suara mereka secara elektronik. Sistem ini dapat mengurangi waktu pemungutan suara, meningkatkan akurasi perhitungan suara, dan meminimalisir potensi kecurangan. Namun, meskipun e-voting menawarkan banyak keuntungan, aspek keamanan menjadi isu utama yang perlu diperhatikan. Keamanan dalam konteks e-voting mencakup berbagai aspek, mulai dari kerahasiaan suara, integritas data, otentikasi pemilih, hingga ketersediaan sistem. Tanpa adanya mekanisme keamanan yang memadai, sistem e-voting rentan terhadap berbagai ancaman, seperti manipulasi suara, serangan siber, dan kebocoran informasi pribadi. Masalah utama yang dihadapi adalah rendahnya keamanan data pada sistem konvensional dan tidak adanya jaminan bahwa data suara pemilih tidak dimanipulasi. Di era digital ini, solusi berbasis teknologi diperlukan untuk mengatasi kendala tersebut.

Penelitian-penelitian yang relevan telah menunjukkan bahwa teknologi e-voting mampu meningkatkan efisiensi dan transparansi. Studi seperti yang dilakukan oleh Rokhman (2011) membahas potensi penerapan e-voting di Indonesia namun mencatat bahwa aspek keamanan data menjadi tantangan utama. Penelitian lain oleh Restu Aji et al. (2023) memperkenalkan blockchain dalam aplikasi e-voting, meskipun implementasinya membutuhkan sumber daya yang besar. Selain itu, Muharram (2018) menunjukkan efektivitas algoritma AES dalam proses enkripsi dan dekripsi, tetapi aplikasinya pada konteks pemilihan belum banyak dibahas secara praktis.

Berdasarkan tantangan dan peluang yang ditemukan, solusi yang diusulkan dalam penelitian ini adalah pengembangan aplikasi e-voting berbasis Android menggunakan algoritma Advanced Encryption Standard (AES) 128-bit. Algoritma AES-128 dipilih karena keandalannya dalam mengamankan data dengan proses enkripsi yang efisien tanpa mengorbankan kinerja sistem.

Rasional pemilihan metode menggunakan algoritma AES-128 adalah karena algoritma ini telah terbukti mampu memberikan keamanan tingkat tinggi dengan waktu pemrosesan yang optimal, sehingga cocok untuk diterapkan pada perangkat dengan sumber daya terbatas seperti smartphone.

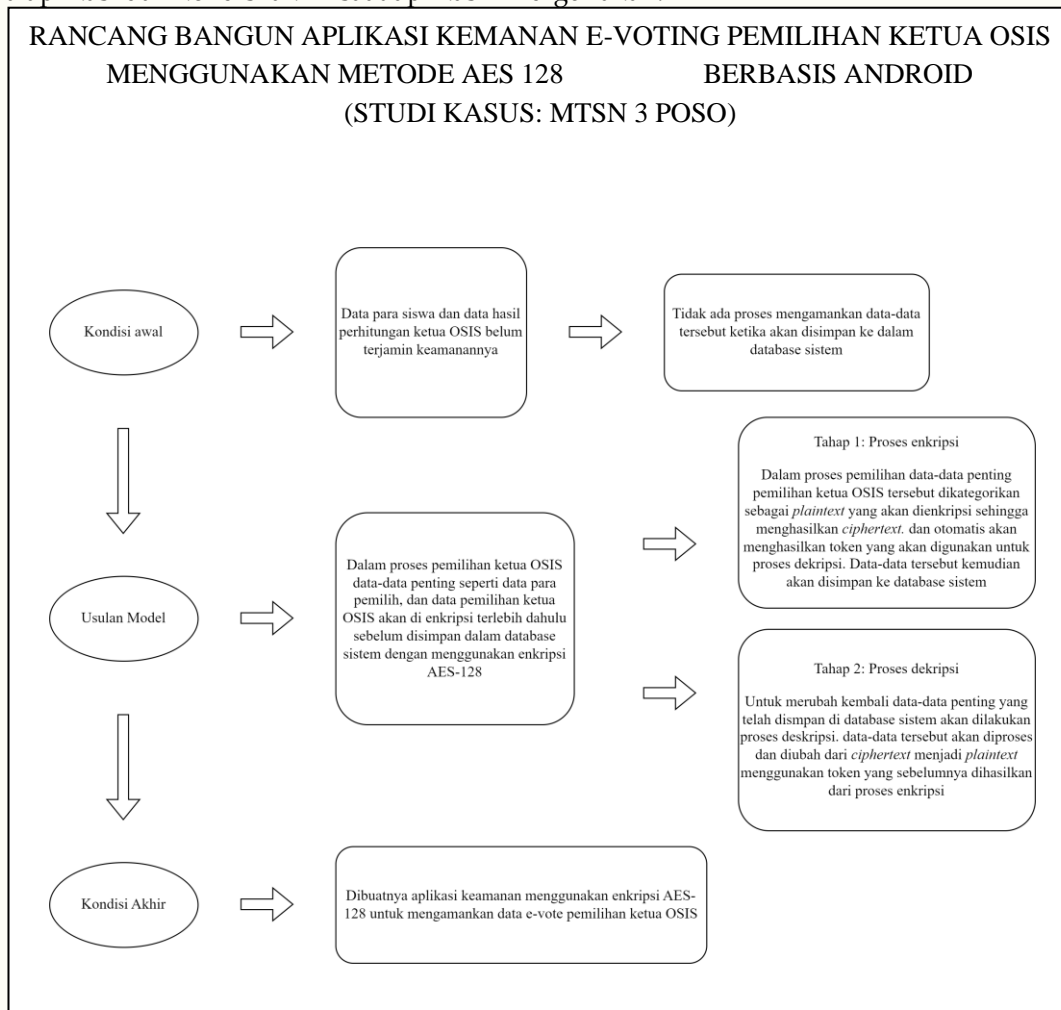
Implementasi berbasis Android juga dipilih karena perangkat ini umum digunakan oleh siswa, sehingga meningkatkan aksesibilitas aplikasi. Dalam ruang lingkup sekolah Organisasi Siswa Intra Sekolah (OSIS) adalah organisasi resmi terbesar di sekolah yang merupakan wadah untuk membina siswa siswa yang diawasi oleh sekolah. Organisasi OSIS terdapat pada sekolah menengah pertama (SMP) dan sekolah menengah atas (SMA), sistem organisasi OSIS terdiri dari berbagai jabatan dan dipimpin oleh ketua dan wakil ketua OSIS dan biasanya dibagi-bagi menjadi beberapa departemen. Ketua dan wakil ketua OSIS dipilih melalui pemilihan selayaknya Pemilu yang diadakan komisioner KPO (Komisi Pemilihan OSIS) yang diikuti oleh seluruh warga sekolah.

Aplikasi ini dibuat bagi siswa agar siswa dapat memberikan suara mereka pada pemilihan ketua OSIS, aplikasi ini dibuat dengan fokus keamanan dan mengatasi masalah-masalah yang sering terjadi pada pemilihan konvensional. Dengan demikian, proses pemilihan dapat berjalan lebih efisien, transparan, dan bebas dari kecurangan.

## METODE

### Kerangka Penelitian

Kerangka penelitian adalah struktur atau rencana yang dirancang untuk memberikan arah yang jelas dan sistematis dalam pelaksanaan suatu penelitian. Kerangka penelitian juga dibuat dengan struktur yang jelas dan rinci agar mudah dipahami oleh pembaca. Kerangka penelitian dari penelitian ini dapat dilihat pada Gambar 1, pada bagian ini akan dideskripsikan perbedaan kondisi awal sebelum aplikasi ini diusulkan, bagaimana usulan model dari aplikasi untuk mengatasi masalah sebelum adanya aplikasi dan kondisi akhir saat aplikasi ini digunakan.



Gambar 1. Kerangka penelitian

Penelitian ini dilakukan untuk mengembangkan aplikasi e-voting berbasis Android dengan algoritma AES-128 untuk keamanan data. Alur penelitian dirancang dalam beberapa tahap utama sebagai berikut:

1. **Identifikasi Masalah**  
Mengidentifikasi kendala dalam pemilihan ketua OSIS secara konvensional, seperti potensi kecurangan, ketidakamanan data, dan ketidakefisienan proses.
2. **Analisis Kebutuhan**  
Menentukan kebutuhan fungsional (input, proses, output) dan non-fungsional (perangkat keras, perangkat lunak, dan kinerja) aplikasi.
3. **Perancangan Sistem**  
Merancang sistem e-voting meliputi antarmuka pengguna, alur data, dan integrasi algoritma enkripsi AES-128 untuk pengamanan.
4. **Implementasi Aplikasi**  
Mengembangkan aplikasi menggunakan Kotlin untuk frontend, Node.js untuk backend, dan MySQL sebagai basis data.
5. **Pengujian dan Evaluasi**  
Menguji aplikasi pada studi kasus pemilihan ketua OSIS di MTsN 3 Poso untuk menilai keandalan sistem dalam pengamanan data suara dan efisiensi proses.

### Penjelasan Alur Penelitian

1. **Identifikasi Masalah**  
Penelitian dimulai dengan analisis sistem pemilihan konvensional yang sering menghadapi masalah, seperti manipulasi data suara, proses yang tidak transparan, dan kesalahan dalam penghitungan suara. Masalah ini menjadi dasar untuk pengembangan aplikasi e-voting yang lebih aman dan efisien.
2. **Analisis Kebutuhan**  
Dilakukan pemetaan kebutuhan aplikasi, baik dari sisi pengguna (panitia dan pemilih) maupun sistem.
  - o *Kebutuhan Fungsional*: Pengelolaan data pemilih, kandidat, dan hasil pemilihan; autentikasi pengguna; dan enkripsi data.
  - o *Kebutuhan Non-Fungsional*: Aplikasi harus berjalan pada perangkat Android dengan spesifikasi minimum RAM 4GB dan prosesor quad-core.
3. **Perancangan Sistem**  
Tahap ini melibatkan desain alur kerja aplikasi, termasuk:
  - o Mekanisme login untuk panitia dan pemilih.
  - o Proses pemilihan berbasis kode QR untuk memastikan satu pengguna hanya dapat memilih sekali.
  - o Implementasi enkripsi AES-128 pada data suara, data kandidat, dan hasil pemilihan untuk keamanan.
4. **Implementasi Aplikasi**  
Aplikasi dikembangkan menggunakan:
  - o *Frontend*: Bahasa pemrograman Kotlin pada Android Studio.
  - o *Backend*: Node.js untuk menangani logika server dan MySQL sebagai database untuk menyimpan data yang dienkripsi.
5. **Pengujian dan Evaluasi**  
Aplikasi diuji pada pemilihan ketua OSIS di MTsN 3 Poso. Pengujian melibatkan:
  - o Uji keamanan: Menguji apakah data suara terenkripsi dengan baik.
  - o Uji fungsionalitas: Memastikan aplikasi berjalan sesuai kebutuhan.

- o Evaluasi efisiensi: Membandingkan waktu dan tingkat kesalahan pemilihan digital dibandingkan metode konvensional.

Dengan alur ini, penelitian berhasil menghasilkan aplikasi e-voting yang aman, efisien, dan transparan.

## Data Penelitian

### Sumber Data

Pada penelitian ini sumber data diperoleh oleh peneliti berupa data dalam wujud primer dan sekunder.

#### a. Data Primer

Data yang dikumpulkan langsung oleh peneliti dari sumber pertama atau asli untuk tujuan penelitian tertentu. Data ini diperoleh melalui metode pengumpulan data yang melibatkan interaksi langsung dengan objek atau subjek yang diteliti. Data primer merupakan sumber data primer merupakan data yang diperoleh secara langsung dari sumber utama (Pramiyati, 2017)

#### b. Data sekunder

Data sekunder adalah data yang telah dikumpulkan oleh orang lain atau lembaga untuk tujuan lain, dan kemudian digunakan kembali oleh peneliti untuk tujuan yang berbeda dari tujuan aslinya. Data ini tersedia dalam bentuk yang telah dipublikasikan atau didokumentasikan. Peneliti melakukan permohonan dan izin yang ditujukan untuk meminta data siswa-siswi pada tempat dilakukannya studi penelitian. Data para siswa tersebut yang akan dijadikan subjek dari penelitian, yang akan menjadi calon kandidat, data suara hak pilih dan data hasil perhitungan perolehan suara pada saat proses pemilihan ketua OSIS. Salah satu contoh data para siswa terdapat pada Tabel 1, tabel tersebut adalah data yang dijadikan sebagai data sekunder untuk penelitian.

Tabel 1. Data Sekunder

No.	Nama Lengkap	NISN	Tempat Lahir	Tanggal Lahir	Jenis Kelamin	Kelas
1	Ferdiansa	3104123805	Mayoa	25072010	Laki-Laki	VIII
2	Mutiara Hikma	3117909090	Malangke	21012011	Perempuan	VIII
3	Safira Ramadani	3096152866	Pandajaya	06122009	Perempuan	VIII
4	Rifka	3106375557	Pinrang	25072010	Perempuan	VIII
5	Misyah Syabila Musyakina	3107420304	Mayoa	08062010	Perempuan	VIII
6	Zhafira Callysta	3109240802	Poso	24032010	Perempuan	VIII
7	Illiyin Nufus	3108202250	Pandajaya	03092008	Perempuan	VIII

## Analisis dan Perancangan

### Kebutuhan Fungsional

Kebutuhan fungsional adalah kebutuhan-kebutuhan tentang fungsi-fungsi yang harus dimiliki oleh suatu sistem untuk memenuhi tujuan dari sistem yang diinginkan. Kebutuhan fungsional harus dapat mengilustrasikan secara terperinci pada masing-masing tingkatan sistem (Kosasi & Margaretha Kuway, 2012). Kebutuhan fungsional dapat dijelaskan dalam 3 hal yaitu kebutuhan jenis masukan, proses-proses yang dibutuhkan, dan luaran yang diharapkan.

#### 1. Kebutuhan masukan

Kebutuhan masukan adalah data atau informasi yang diperlukan oleh sistem untuk melakukan fungsi-fungsi yang diinginkan. Dalam penelitian ini kebutuhan masukan dijabarkan pada Tabel 2 sebagai berikut:

Tabel 2. Kebutuhan Masukan

No.	Entitas	Kebutuhan Masukan
1.	Panitia	<ul style="list-style-type: none"> <li>• Panitia melakukan input data email dan kata sandi untuk melakukan proses login.</li> <li>• Lembaga independen melakukan input data pemilih yang akan menggunakan hak pilihnya.</li> <li>• Panitia melakukan input data calon kandidat ketua OSIS.</li> <li>• Panitia melakukan input data pemilihan untuk proses pemilihan ketua OSIS.</li> </ul>
2.	Pemilih	<ul style="list-style-type: none"> <li>• Pemilih melakukan input data email dan kata sandi untuk melakukan proses login.</li> <li>• Pemilih melakukan input data suara untuk menggunakan hak pilih pada proses pemilihan.</li> </ul>

2. Kebutuhan proses

Kebutuhan proses adalah langkah-langkah atau operasi yang dilakukan oleh sistem untuk mengolah masukan menjadi hasil yang diinginkan. Dalam penelitian ini kebutuhan proses dijabarkan pada Tabel 3. sebagai berikut:

Tabel 3. Kebutuhan Proses

No.	Entitas	Kebutuhan Proses
1.	Panitia	<ul style="list-style-type: none"> <li>• Panitia dapat melakukan proses login.</li> <li>• Panitia dapat melihat profil visi misi calon kandidat.</li> <li>• Panitia dapat melihat data warga pemilih.</li> <li>• Panitia dapat membuat jadwal pemilihan.</li> <li>• Panitia dapat memasukkan data para calon kandidat</li> <li>• Panitia dapat melihat data para pemilih.</li> <li>• Panitia dapat melihat data hasil suara.</li> </ul>
2.	Pemilih	<ul style="list-style-type: none"> <li>• Pemilih dapat melakukan proses login.</li> <li>• Pemilih dapat melakukan proses pemilihan kandidat ketua dan wakil ketua</li> <li>• Pemilih dapat memasukkan kode PIN untuk verifikasi saat akan melakukan proses pemilihan.</li> <li>• Pemilih dapat melihat data kandidat kepala desa.</li> <li>• Pemilih dapat melihat hasil suara pemilihan</li> </ul>

3. Kebutuhan luaran

Kebutuhan luaran adalah hasil akhir yang dihasilkan oleh sistem setelah melakukan pemrosesan. Dalam penelitian ini kebutuhan luaran dijabarkan pada Tabel 4 sebagai berikut:

Tabel 4. Kebutuhan Luaran

No.	Entitas	Kebutuhan luaran
1.	Panitia	<ul style="list-style-type: none"> <li>• Panitia membuat laporan dan mencetak laporan hasil pemilihan</li> </ul>
2.	Pemilih	<ul style="list-style-type: none"> <li>• Para pemilih melihat hasil laporan dari hasil pemilihan</li> </ul>

**Kebutuhan non fungsional**

Kebutuhan non-fungsional adalah kebutuhan dari suatu sistem yang menentukan bagaimana sistem tersebut beroperasi. Kebutuhan ini mencakup karakteristik dan sifat sistem yang mempengaruhi pengalaman pengguna serta kinerja dan efisiensi sistem. Kebutuhan non-fungsional lebih mengarah kepada batasan layanan atau fungsi yang diberikan sistem (Kosasi & Margaretha Kuway, 2012).

1. Kebutuhan perangkat lunak

Pada penelitian ini untuk membuat sistem diperlukan perangkat lunak sebagai berikut:

- a. Android Studio
  - b. MySql
  - c. Xampp
  - d. Visual studio code
  - e. Figma
2. Kebutuhan perangkat keras

Untuk membuat sistem diperlukan perangkat keras sebagai berikut:

Tabel 5. Kebutuhan Perangkat Keras

Smartphone	Prosesor: Quad-core
	RAM: 4GB
	Penyimpanan: 64GB
	OS: Android 8.0 (Oreo)
	Memory: 8GB
Laptop	Processor : Intel i3 10300U
	OS : Windows 11 Home
	GPU : NVIDIA GTX 930M
	VGA : Intel(R) HD Graphics

## HASIL DAN PEMBAHASAN

### Hasil

Hasil dari penelitian ini adalah sebuah aplikasi keamanan e-voting pemilihan ketua OSIS berbasis android yang dibuat dengan menggunakan enkripsi algoritma AES-128. Aplikasi ini dibuat berdasarkan masalah-masalah yang sering dihadapi dalam pemilihan konvensional seperti tindakan kecurangan. Aplikasi ini dibuat dengan menggunakan bahasa pemrograman kotlin untuk membuat bagian *frontend* yang digunakan sebagai alat bantu untuk pembuatan dan pengembangan aplikasi. Aplikasi ini menggunakan *framework* Node.js untuk bagian *backend*. Untuk menyimpan data pemilihan aplikasi ini menggunakan MySql sebagai *database*. Aplikasi e-voting ini memiliki kelebihan dari aplikasi e-voting lainnya pada fitur keamanan, dikarenakan aplikasi ini dibuat dengan menggunakan algoritma AES-128 bit data-data selama proses pemilihan seperti data suara, data pemilih dan hasil suara dari proses pemilihan akan melewati tahap enkripsi dan dekripsi, yang membuat data-data penting tersebut sudah terjamin keamanannya. Juga terdapat keamanan bawaan dari android studio berupa algoritma class Chiper yang merupakan bawaan langsung dari aplikasi tersebut.

Aplikasi ini dibuat dan digunakan berdasarkan studi kasus yakni diruang lingkup dari sekolah MTsN 3 Poso, yang digunakan untuk melakukan proses pemilihan ketua dan wakil ketua OSIS pada sekolah tersebut. Aplikasi ini digunakan oleh dua entitas utama yaitu pemilih dan panitia atau admin. Admin memiliki hak akses utama untuk membuat data kandidat ketua dan wakil ketua OSIS, membuat jadwal pemilihan yang juga termasuk membuat kode QR pemilihan. Entitas pemilih, memiliki hanya memiliki akses untuk melakukan proses pemilihan suara atau voting dan melihat hasil suara pemilihan. Cara kerja dari aplikasi ini yaitu, pada saat dilakukan proses pemilihan atau voting pemilihan akan dilakukan oleh para pemilih dengan memindai kode QR yang dihasilkan oleh panitia. Jika kode QR sesuai, maka pemilih baru akan bisa melakukan proses pemilihan. Jika pemilih telah memilih sebelumnya maka pemilih tidak dapat melakukan pemilihan lagi dan kode QR tersebut akan dibaca tidak valid oleh sistem aplikasi. Data suara yang telah masuk kedalam sistem akan diproses dengan mengenkripsi data suara tadi dengan menggunakan algoritma AES-128. Selain itu, data penting yang lain seperti data pemilih, dan data kandidat juga dilakukan proses enkripsi dengan menggunakan AES-128.

Berikut adalah contoh penerapan dari algoritma AES-128 dalam aplikasi yang dibuat.

```
const crypto = require('crypto')
function adjustKey(key) {
  if (key.length < 16) {
    return key.padEnd(16, '0'); // Padding dengan '0' jika kurang dari 16 karakter
  }
  return key.substring(0, 16); // Memotong jika lebih dari 16 karakter
}
// Fungsi untuk mengenkripsi teks dengan AES-128
exports.encrypt = (text, userKey)=> {
  const key = Buffer.from(adjustKey(userKey), 'utf8');
  const iv = crypto.randomBytes(16); // Inisialisasi vektor
  const cipher = crypto.createCipheriv('aes-128-cbc', key, iv);
  let encrypted = cipher.update(text, 'utf8', 'hex');
  encrypted += cipher.final('hex');
  return iv.toString('hex') + ':' + encrypted;
}
```

Gambar 1. Implementasi Enkripsi Algoritma AES-128

```
// Fungsi untuk mendekripsi teks dengan AES-128
exports.decrypt = (text, userKey)=>{
  const key = Buffer.from(adjustKey(userKey), 'utf8');
  const textParts = text.split(':');
  const iv = Buffer.from(textParts.shift(), 'hex');
  const encryptedText = textParts.join(':');
  const decipher = crypto.createDecipheriv('aes-128-cbc', key, iv);
  let decrypted = decipher.update(encryptedText, 'hex', 'utf8');
  decrypted += decipher.final('utf8');
  return decrypted;
}
```

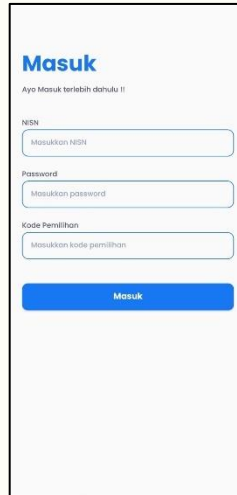
Gambar 2. Implementasi Dekripsi Algoritma AES-128

## Pembahasan

Pembahasan hasil dari penelitian ini adalah sebagai berikut.

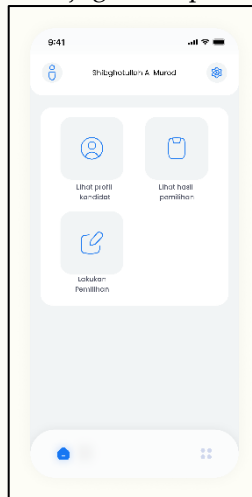
1. Pada Gambar 3. dibawah terdapat tampilan masuk akun yang digunakan oleh panitia, dan pemilih untuk masuk ke dalam aplikasi. Pemilih harus memasukkan NISN, kata sandi dan kode pemilihan untuk masuk. Sedangkan panitia harus memasukkan email, kata sandi dan kode pemilihan untuk verifikasi. Jika data yang dimasukkan benar, maka pengguna akan masuk ke halaman utama.





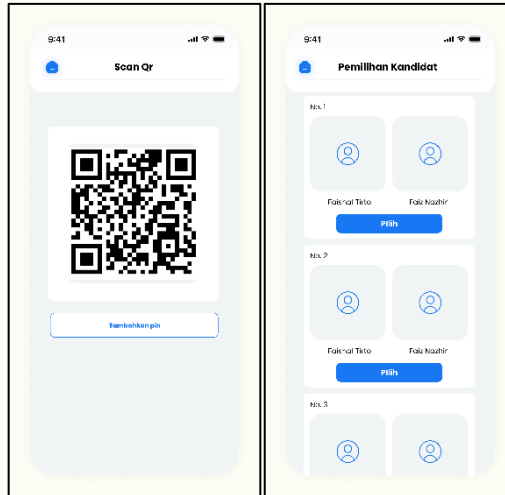
Gambar 3. Tampilan Masuk Akun

2. Pada Gambar 4. terdapat tampilan halaman utama pemilih yang berisi menu lihat profil kandidat, lihat hasil pemilihan, dan menu untuk melakukan pemilihan. Halaman utama ini dapat diakses oleh pemilih setelah melakukan login. Selain itu, juga terdapat sebuah tombol untuk melakukan voting.



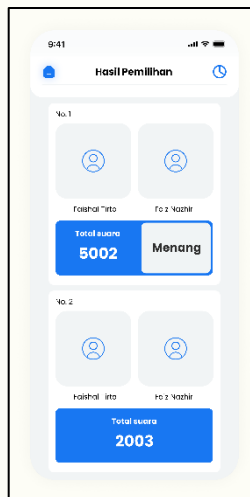
Gambar 4. Tampilan Menu Utama Pemilih

3. Pada Gambar 5 terdapat tampilan pilih calon kandidat yang digunakan oleh pemilih untuk melakukan proses pemilihan calon kandidat Ketua OSIS. Saat akan melakukan proses pemilihan, pemilih harus memindai kode QR atau memasukkan text kode QR secara manual. Jika QR code berhasil diverifikasi, maka pemilih akan diberikan tampilan daftar kandidat calon Ketua OSIS.



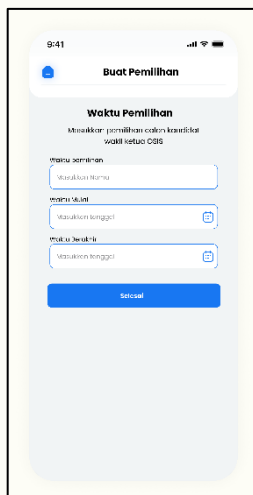
Gambar 5. Tampilan Proses Memilih Calon Kandidat

4. Pada Gambar 6 terdapat tampilan lihat hasil pemilihan yang bisa diakses oleh pemilih dan panitia untuk melihat hasil pemilihan kepala desa. Pada halaman ini pemilih bisa melihat total hasil suara yang diperoleh oleh setiap kandidat Ketua dan wakil ketua OSIS. Hasil pemilihan akan ditampilkan sesuai suara yang masuk, dan bagi calon kandidat dengan suara terbanyak akan ditampilkan sebagai pemenang pada aplikasi.



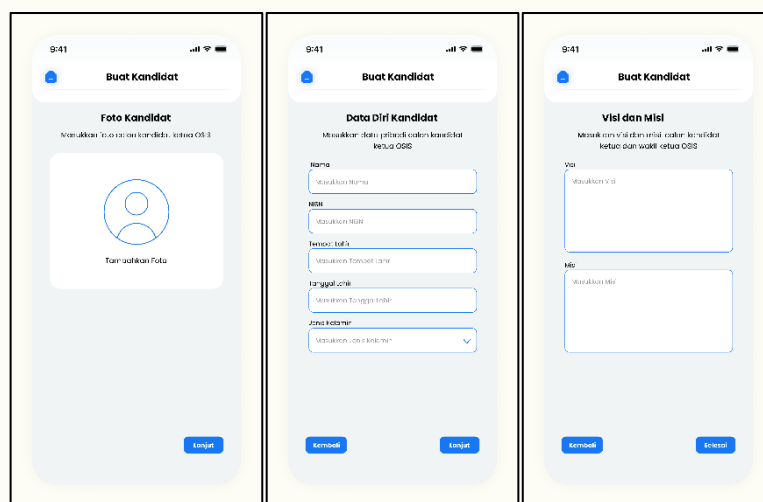
Gambar 1. Tampilan Lihat Hasil Pemilihan

5. Pada Gambar 7 terdapat tampilan halaman buat pemilihan baru yang dapat diakses oleh panitia untuk membuat pemilihan ketua OSIS. Untuk membuat pemilihan baru panitia harus memasukkan tanggal, waktu mulai, dan waktu berakhirnya pemilihan.



Gambar 7. Tampilan Buat Pemilihan Baru

6. Pada Gambar 8 terdapat tampilan halaman membuat kandidat ketua OSIS yang diakses dan diisi oleh panita. Untuk membuat kandidat kepala desa perlu memasukkan data-data kandidat terkait proses pemilihan ketua OSIS seperti foto, nama, tempat tanggal lahir, jenis kelamin, serta visi dan misi.



Gambar 8. Tampilan Buat Pemilihan Baru

Penelitian ini menghasilkan sebuah aplikasi e-voting berbasis Android yang menggunakan algoritma enkripsi AES-128 untuk menjamin keamanan data. Dalam implementasinya, data penting seperti data suara, data pemilih, dan hasil pemilihan dienkripsi sebelum disimpan atau diproses. Hal ini bertujuan untuk memastikan bahwa data tersebut tetap aman dari ancaman manipulasi atau pencurian. Sebagai contoh penerapan enkripsi menggunakan AES-128, berikut ditampilkan hasil enkripsi dari data teks (plaintext) menjadi ciphertext. Data teks yang digunakan adalah data suara pemilih, yang dienkripsi menggunakan kunci tertentu. Hasil dari proses enkripsi dapat dilihat pada Tabel berikut:

Tabel 6. Hasil Proses Enkripsi

No.	Plaintext	Key (16 karakter)	Ciphertext
1	Pilihan: Kandidat A	mysecurekey123456	7e4a9b8f1c34d0d4f8b9a6c7e3f5210a
2	Pilihan: Kandidat B	mysecurekey123456	3d7c9fbe6a34b6f2a89c123fdc89ab12

No.	Plaintext	Key (16 karakter)	Ciphertext
3	Pilihan: Kandidat C	mysecurekey123456	5b1a7c4d8e3f9f6c7b4a1234de89f01a

Tabel ini menunjukkan bahwa setiap plaintext (data awal) berhasil dikonversi menjadi ciphertext (hasil enkripsi) dengan algoritma AES-128 menggunakan kunci enkripsi sepanjang 16 karakter. Ciphertext tersebut tidak dapat dibaca tanpa proses dekripsi menggunakan kunci yang sama. Hasil ini membuktikan bahwa algoritma AES-128 mampu menjaga kerahasiaan data selama proses pemilihan berlangsung. Dengan adanya fitur ini, aplikasi e-voting memastikan bahwa data suara tetap aman, bahkan jika terjadi akses tidak sah pada basis data aplikasi.

## KESIMPULAN

Penelitian ini berhasil menciptakan aplikasi keamanan e-voting untuk data pemilihan ketua OSIS dengan menggunakan algoritma AES-128. Aplikasi ini berhasil mengatasi beberapa masalah yang sering terjadi pada pemilihan konvensional. Aplikasi ini dapat mewujudkan asas pemilu yaitu langsung, umum, bebas, rahasia, jujur, dan adil dengan mengamankan data-data penting pada proses pemilihan ketua OSIS seperti data pemilihan, data kandidat ketua dan wakil ketua OSIS, dan data hasil pemilihan serta perolehan hasil suara. Dengan algoritma AES-128 data-data penting tersebut diamankan dengan baik. Berdasarkan penelitian tentang aplikasi keamanan e-voting menggunakan algoritma AES-128, terdapat berbagai peluang untuk pengembangan lebih lanjut. Penelitian selanjutnya dapat difokuskan pada pengadopsian algoritma keamanan yang lebih canggih, seperti AES-256 atau blockchain, untuk meningkatkan perlindungan data. Selain itu, implementasi aplikasi dalam skala yang lebih besar, seperti pemilu tingkat universitas atau komunitas, dapat menjadi langkah penting untuk menguji keandalan sistem. Pengintegrasian teknologi biometrik, seperti pemindai sidik jari atau pengenalan wajah, juga dapat meningkatkan otentikasi pengguna dan mencegah penyalahgunaan sistem. Penelitian tambahan yang mengevaluasi risiko serangan siber serta analisis biaya dan efisiensi operasional dapat membantu memperkuat keandalan dan efektivitas aplikasi. Dengan mengembangkan aplikasi agar kompatibel dengan berbagai platform dan menyesuaikannya untuk skala pemilu nasional, aplikasi ini memiliki potensi untuk menjadi solusi inovatif dalam proses pemilihan yang aman, efisien, dan transparan.

## DAFTAR PUSTAKA

- Abdurahman, H., Riswaya, A. R., & Id, A. (2014). Aplikasi pinjaman pembayaran secara kredit pada bank yudha bhakti. *Jurnal Computech & Bisnis*, 8(2), 61-69.
- Aji, S. R., & Putri, W. T. H. (2023). Implementasi Teknologi Blockchain dalam Aplikasi E-Voting Berbasis Mobile. *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, 14(2), 219-231. <https://doi.org/10.31849/Digitalzone.V14i2.16682>
- Arif, A. (2021). Penerapan Metode Extreme Programming Pada E-Voting Pemilihan Ketua Unit Kegiatan Mahasiswa (Ukm) Sekolah Tinggi Teknologi Xyz. *Jurnal Sistem Dan Teknologi Informasi (Justin)*, 9(2), 234. <https://doi.org/10.26418/Justin.V9i2.44266>
- Aunur, R. Mulyanto, 2008. *Rekayasa Perangkat Lunak Jilid 1 Untuk Smk*, Departemen Pendidikan Nasional, 2008.
- Gultom, M. M. I., & Saripurna, D. (2019). Perancangan Sistem Keamanan Aplikasi E-Voting Untuk Pemilihan Ketua Badan Eksekutif Mahasiswa Fakultas Teknik UISU Dengan Menggunakan Algoritma MD5. *Algoritma: Jurnal Ilmu Komputer Dan Informatika*, 3(2), 70. <http://dx.doi.org/10.30829/algoritma.v3i2.6438>

- Hasugian, H., & Shidiq, A. N. (2012). Rancang bangun sistem informasi industri kreatif bidang penyewaan sarana olahraga. *Semantik 2012*, 606-616.
- Hendini, A. (2016). Pemodelan UML sistem informasi monitoring penjualan dan stok barang (studi kasus: distro zhezha pontianak). *Jurnal Khatulistiwa Informatika*, 4(2).
- Hermawati, F. D., Tahir, M., Syaifurrohman, M., Hikmah, M., Amroin, J. A., Bahruddin, M., & Irsyad, I. (2023). Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard). *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, 2(2), 45-56. <https://doi.org/10.55606/jtmei.v2i2.1625>
- Hu, S. D. K., Palit, H. N., & Handoyo, A. (2019). Implementasi Blockchain: Studi Kasus e-Voting. *Jurnal Infra*, 7(1), 183-189.
- Jocelyn A.J. Evans. (2004). *Voters And Voting*. Sage Publications.
- Juansyah, A. (2015). Pembangunan aplikasi child tracker berbasis assisted–global positioning system (a-gps) dengan platform android. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, 1(1), 1-8.
- Kosasi, S., & Kuway, S. M. (2012). Studi Analisis Persyaratan Kebutuhan Sistem Dalam Menghasilkan Perangkat Lunak Yang Berkualitas. *Sisfotenika*, 2(1), 1-10.
- Latukolan, M. L. A., Arwan, A., & Ananta, M. T. (2019). Pengembangan Sistem Pemetaan Otomatis Entity Relationship Diagram Ke Dalam Database. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 3(4), 4058-4065.
- Muharram, F., Aziz, H., & Manga, A. R. (2018, September). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). In *Prosiding SAKTI (Seminar Ilmu Komputer dan Teknologi Informasi)* (Vol. 3, No. 2, pp. 112-115).
- Pramiyati, T., Jayanta, J., & Yulnelly, Y. (2017). Peran Data Primer Pada Pembentukan Skema Konseptual Yang Faktual (Studi Kasus: Skema Konseptual Basisdata Simbumil). *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, 8(2), 679-686. <https://doi.org/10.24176/simet.v8i2.1574>
- Rokhman, A. (2011, July). Prospek dan tantangan penerapan e-voting di indonesia. In *Seminar Nasional Peran Negara dan masyarakat dalam Pembangunan Demokrasi dan Masyarakat madani di indonesia* (Vol. 7, pp. 1-11).
- Risnanto, S. (2018). Aplikasi Pemungutan Suara Elektronik / E-Voting Menggunakan Teknologi Short Message Service Dan At Command. *Jurnal Teknik Informatika*, 10(1), 17–26. <https://doi.org/10.15408/Jti.V10i1.6811>
- Yuniati, V., & Indriyanta, G. (2011). Enkripsi dan dekripsi dengan algoritma aes 256 untuk semua jenis file. *Jurnal Informatika*, 5(1).