

## Penerapan Metode Enkripsi Base64, SHA-512 DAN AES Untuk Menjamin Sebuah Keabsahan Ijazah

Arya Fajar Siswanto<sup>1)</sup>, Agus Herwanto<sup>2)</sup>, Malabay<sup>3)</sup>, Holder Simorangkir<sup>4)</sup>

Program Studi Teknik Informatika, Universitas Esa Unggul, Bekasi

E-mail: <sup>1)</sup>aryatgtsfs@gmail.com, <sup>2)</sup>agus.herwanto@esaunggul.ac.id, <sup>3)</sup>malabay@esaunggul.ac.id, <sup>4)</sup>holder@esaunggul.ac.id

### ABSTRAK

Keamanan memiliki peran yang krusial dalam berbagai aspek kehidupan, terutama seiring dengan kemajuan teknologi dan informasi. Munculnya berbagai tindak kejahatan baru menekankan perlunya peningkatan keamanan salah satunya adalah pemalsuan ijazah. Pemalsuan Ijazah adalah salah satu bentuk kejahatan yang rentan. Penelitian ini bertujuan mengembangkan aplikasi validasi ijazah dengan fokus pada pengesahan yang dapat dipertanggungjawabkan. Aplikasi ini menggunakan metode waterfall sebagai kerangka kerja pengembangan dan teknologi Optical Character Recognition (OCR) untuk mengubah data dari gambar ijazah menjadi teks. Data yang didapatkan nanti akan dibandingkan dengan informasi yang dimasukkan oleh pengguna pada aplikasi yang akan dibuat. Setelah itu, tiga algoritma enkripsi yaitu Base64, AES, dan SHA-512 yang akan diterapkan pada server dimana tiga algoritma tersebut akan berperan besar pada keamanan data ijazah di database. Pengembangan aplikasi ini menggunakan bahasa pemrograman Dart (framework Flutter) untuk pembuatan aplikasi seluler dan JavaScript (framework NodeJs) untuk server. Penelitian ini menggabungkan tiga algoritma untuk menjaga integritas ijazah dengan lebih efektif dan menjadikannya lebih absah.

**Kata Kunci:** Enkripsi, Base64, SHA-512, AES

### ABSTRACT

*Security has a crucial role in various aspects of life, especially in line with advances in technology and information. The emergence of various new crimes emphasizes the need for increased security, one of which is the forgery of diplomas. Diploma forgery is a form of crime that is vulnerable. This study aims to develop diploma validation applications with a focus on validation that can be accounted for. This application uses the waterfall method as a development framework and Optical Character Recognition (OCR) technology to convert data from diploma images into text. The data obtained will be compared with the information entered by the user in the application to be made. After that, three encryption algorithms namely Base64, AES, and SHA-512 will be applied to the server where these three algorithms will play a major role in the security of diploma data in the database. The development of this application uses the Dart programming language (Flutter framework) for mobile application development and JavaScript (NodeJs framework) for servers. This research combines three algorithms to more effectively maintain the integrity of diplomas and make them more valid.*

**Keyword:** Encryption, Base64, SHA-512, AES

## 1. PENDAHULUAN

### Latar Belakang

Ijazah merupakan suatu dokumen yang berisi tentang pengakuan yang diberikan oleh instansi terkait atas keberhasilan seseorang dalam masa pembelajarannya. Dimana dalam penggunaannya ijazah bisa dilampirkan dalam bentuk salinan kemudian dilegalisasi oleh instansi terkait untuk membuktikan keaslian dari ijazah tersebut. Masyarakat saat ini dihadapkan pada tantangan keamanan yang berkembang seiring dengan munculnya berbagai bentuk kejahatan baru yang sulit dideteksi dan dicegah. Salah satu bentuk kejahatan yang semakin mengkhawatirkan adalah pemalsuan ijazah.

Fenomena ini mencerminkan dampak negatif dari perkembangan teknologi, di mana orang dengan niat buruk dapat dengan mudah memalsukan dokumen penting seperti ijazah. Pemalsuan ijazah menjadi masalah serius karena tidak hanya merugikan lembaga pendidikan dan pihak yang mempekerjakan, tetapi juga mengancam kepercayaan dalam sistem pendidikan dan dunia kerja. Penyalahgunaan ijazah pada umumnya bukan hanya dilakukan oleh orang-orang biasa saja, tetapi tidak menutup kemungkinan terjadi pada kalangan pejabat publik (Aziz, 2018).

Untuk menjamin keabsahan dokumen diperlukan adanya tempat untuk memvalidasi dan menjamin keaslian dokumen tersebut. Selain itu diperlukan adanya keamanan agar data tersebut tidak bisa dirubah oleh pihak lain. Oleh sebab itu penelitian ini bertujuan untuk merancang dan mengembangkan sebuah aplikasi seluler berbasis framework Flutter yang memfasilitasi validasi keabsahan ijazah.

Aplikasi ini akan memberikan Universitas Esa Unggul dan pihak yang berkepentingan kemampuan untuk memverifikasi keaslian sebuah ijazah. Metode enkripsi seperti base64, SHA-512, dan AES akan diterapkan untuk memastikan bahwa informasi yang disimpan dalam ijazah tetap aman dan tidak dapat dimanipulasi.

Dengan adanya solusi ini, diharapkan Universitas Esa Unggul dapat mempertahankan kepercayaan masyarakat dalam integritas ijazah, serta mencegah penyalahgunaan dan pemalsuan dokumen yang merugikan. Melalui aplikasi ini, proses validasi keabsahan ijazah akan menjadi lebih efisien dan akurat,

memberikan manfaat besar bagi semua pihak yang terlibat.

### Identifikasi Masalah

1. Belum tersedia suatu aplikasi untuk membuktikan keabsahan ijazah.
2. Belum tersedia kewanitaan untuk tidak disalahgunakan oleh pihak lain.
3. Bagaimana membuat keamanan yang ringan, mudah diakses dan terjamin datanya.

### Tujuan

1. Membangun aplikasi validasi ijazah.
2. Menyediakan wadah untuk pihak kampus untuk mengakses aplikasi dengan mudah.
3. Membuat sistem keamanan yang ringan dan terjamin datanya.

## 2. KAJIAN PUSTAKA

### Kriptografi

Kriptografi adalah sebuah metode yang digunakan untuk memproteksi data asli dengan metode mengubah data asli (*plaintext*) menjadi data yang sangat berbeda dengan data asli (*ciphertext*). Namun, data yang berbeda dari data asli tersebut (*ciphertext*) bisa dirubah lagi menjadi data asli (*plaintext*). Pada penelitian ini peneliti menggunakan 3 algoritma kriptografi untuk mengamankan dokumen. Antara lain:

1. **Base64**  
Algoritma Base64 adalah algoritma yang mengubah data dengan cara memecah setiap 3 byte data biner menjadi 4 blok karakter ASCII String. Algoritma ini menggunakan 64 karakter yang diambil dari A-Z (Huruf besar dan kecil), 0-9, simbol '/' dan simbol '+', yang akhirnya diakhiri dengan menambahkan karakter '=' jika data bukan kelipatan 3.
2. **SHA-512**  
SHA-512 sering disebut juga dengan *Secure Hash Algorithm 512-bit* adalah algoritma yang biasanya digunakan untuk menyamakan hasil akhir dan tidak bisa dilakukan hasil pembalik (decrypt). Cara kerjanya data dipecah menjadi blok data yang mempunyai ukuran 1024 bit, lalu digunakan perhitungan matematis pada

tiap blok data sampai hasilnya menghasilkan nilai hash 512-bit.

### 3. AES

*Advanced Encryption Standard* atau disingkat AES adalah algoritma simetri dimana kunci yang digunakan untuk proses enkripsi dan deskripsi sama (Halim & Sugiarto, 2018). Cara kerjanya mengganti dan menggeser blok data yang didasarkan pada kunci. Kunci pada AES dapat memiliki panjang 128-bit, 192-bit dan 256-bit.

### Kode QR

Kode Qr tidak lain tidak bukan adalah bentuk dari revolusi barcode yang sering kita lihat dibungkus produk. Kode QR berbentuk jajaran persegi yang umunya berwarna putih dan hitam.

Kode Qr dapat menyimpan banyak data seperti numerik, alphanumeric sampai kanji. Selain itu, Kode Qr dapat dibaca dari berbagai sudut dikarenakan terdapat tiga tanda berbentuk persegi di tiga sudut sebagai pembatas kode (Firdaus, Yusuf Nur Ikhsan, 2022). Oleh karena itu, kode qr sangat membantu dalam menyimpan kode yang rumit namun tidak terlalu banyak karena akan mengurangi akurasi saat proses membacanya.

### OCR

*Optical Character Recognition* atau teknologi OCR adalah teknologi yang digunakan untuk mengenali, mengidentifikasi, dan mengubah teks yang tercetak atau ditulis tangan menjadi format yang dapat diolah oleh komputer. Dalam istilah sederhana, OCR memungkinkan komputer untuk 'membaca' atau mengenali teks dari gambar atau dokumen yang telah dipindai atau difoto, sehingga memungkinkan pengguna untuk mengedit, mencari, atau menggandakan isi teks tersebut.

### Framework Flutter

Flutter adalah kerangka kerja sumber terbuka yang dibesarkan oleh Google. Framework Flutter digunakan untuk membangun aplikasi seluler (mobile) dan aplikasi web dari satu kode basis yang sama. Dengan menggunakan bahasa pemrograman Dart, Flutter memungkinkan pengembang untuk menciptakan antarmuka pengguna yang kaya dan menarik dengan cepat dan mudah.

Eksperimen yang dilakukan menggunakan flutter sangat cepat dan mudah seperti membuat UI, menambahkan fitur-fitur yang diperlukan dan memperbaiki bug (Ernawati et al., 2021).

### 3. METODE PENELITIAN

Penelitian bertujuan untuk membuat sebuah aplikasi yang mampu untuk menjamin kode Qr yang dihasilkan oleh aplikasi ini. Aplikasi ini juga memungkinkan user instansi Universitas Esa Unggul agar dapat mengajukan permintaan validasi dan dapat disetujui permintaan validasi tersebut oleh seseorang yang berwenang dan bisa diminta pertanggung jawabannya. Selain itu, data yang sudah tervalidasi dapat dijaga dengan algoritma yang rumit didatabase. Sehingga data yang disimpan di database bisa dijamin keamanannya.

Metode penelitian yang digunakan oleh penulis adalah metode air terjun atau sering disebut *waterfall*. Metode ini dinamakan air terjun karena karakteristiknya yaitu sistematis dan berurutan yang bertujuan untuk kemudahan dalam pengelolaan (Malabay et al., 2022). Pada langkah-langkahnya metode ini mempunyai urutan yaitu

#### A. Analisis kebutuhan

Pada proses ini diadakan analisis kebutuhan untuk dapat menentukan batas dan apa saja yang dibutuhkan sebelum mengimplementasikan perangkat lunak dilakukan.

#### B. Desain sistem

Langkah selanjutnya representasi desain sistem yang diharapkan dapat diimplementasikan secara utuh sebagai perangkat lunak pada tahap implementasi (Asmarajaya et al., 2021). Pada tahap ini dirancang sebuah *Activity Diagram* untuk dapat memudahkan alur logika.

#### C. Implementasi

Langkah selanjutnya adalah pengimplementasian sebuah desain aplikasi dari sebuah desain sistem menuju ke perangkat lunak (*coding*) dalam penelitian ini aplikasi mobile

#### D. Integrasi pengujian

Pada langkah ini dilakukan uji coba agar aplikasi yang dibuat dapat berjalan dengan lancar sesuai dengan analisis kebutuhan

**E. Pemeliharaan**

Pada tahap ini diberikan kepada pengguna dan dilakukan proses pemeliharaan

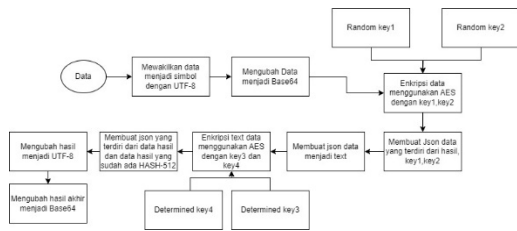
**4. HASIL DAN PEMBAHASAN**

**Analisis Kebutuhan**

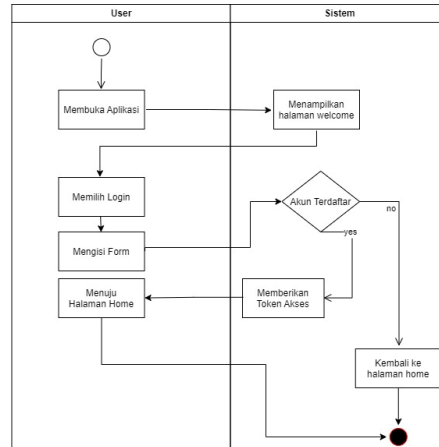
Dalam melaksanakan penelitian terdapat sebuah keperluan dari dalam kampus dimana diperlukannya sebuah tempat Validasi Ijazah dimana didalamnya masyarakat Universitas Esa Unggul dapat mengajukan ijazah untuk divalidasi oleh pihak yang berwenang dan bukti validasi tersebut dapat dibawa kemanapun dengan berbentuk Kode Qr yang bisa diunduh lalu dibuat keamanan yang rumit ketika ingin menyimpan di database.

**Desain Sistem**

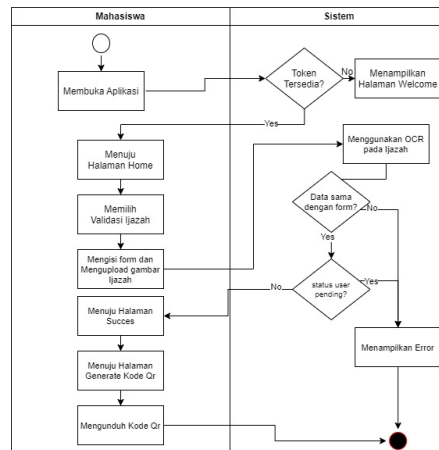
Dikarenakan sistem hanya berorientasi pada kegunaan maka diperlukan *Activity Diagram*. *Activity Diagram* digunakan untuk menunjukan aliran logika pada suatu aktifitas aplikasi. Untuk dapat memudahkan dalam pengimplementasian aplikasi maka dibuatlah 3 *Activity Diagram* untuk *Backend* dan 3 *Activity Diagram* untuk *Frontend* sebagai berikut:



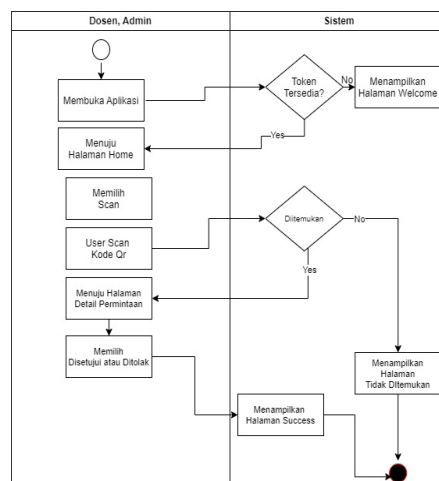
Gambar 1: Alur Enkripsi 50%



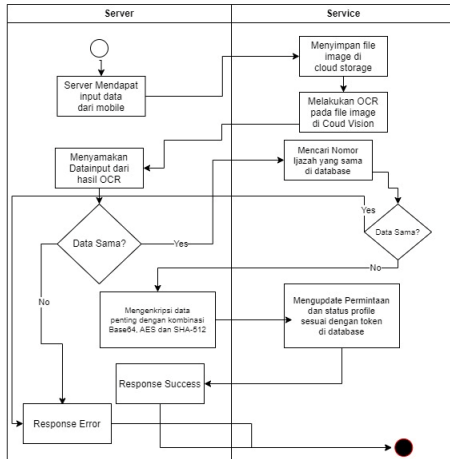
Gambar 2: Activity Login



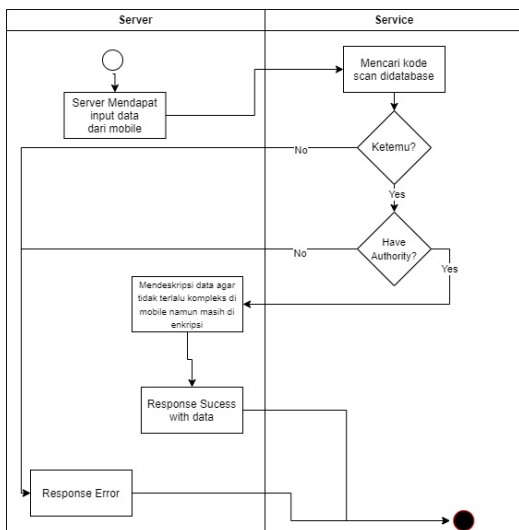
Gambar 3: Activity Permintaan Validasi



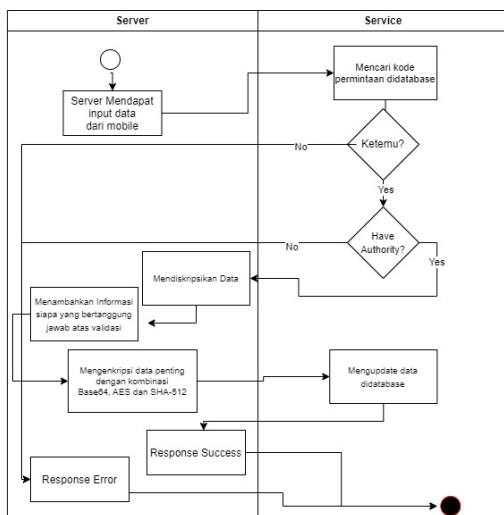
Gambar 4: Activity Validasi Permintaan



Gambar 5: Activity Validasi Sertifikat Backend



Gambar 6: Activity Scan Backend



Gambar 7: Activity Validasi

## Implementasi

Implementasi adalah sebuah hasil yang sudah dibangun berdasarkan desain sistem pada tahap sebelumnya. Implementasi yang dibangun memuat halaman *welcome*, *login*, *home*, validasi ijazah, *success*, *generate qr code*, *scan*, detail *request* dan validasi *success*.



Esascan

Makin Mudah Makin Cepat  
Aplikasi untuk Validasi Ijazah, Izin dan Tanda Tangan QrCode



Gambar 8: Halaman Welcome



Masuk



E-mail/No.Induk

emailkamu@gmail.com

Kata Sandi

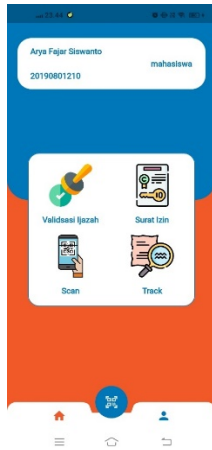
Kata Sandi

Masuk

Belum punya akun? Daftar



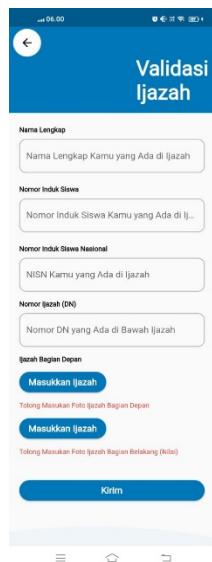
Gambar 9: Halaman Login



Gambar 10: Halaman *Home*



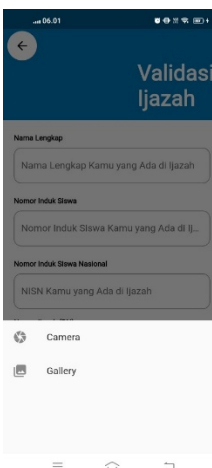
Gambar 13: Halaman *Success*



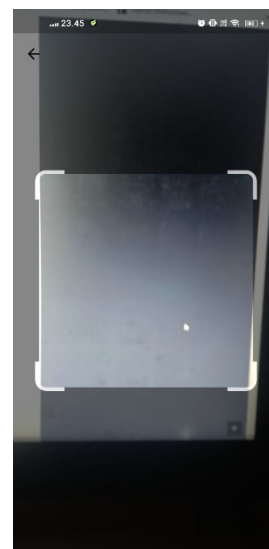
Gambar 11: Validasi Ijazah



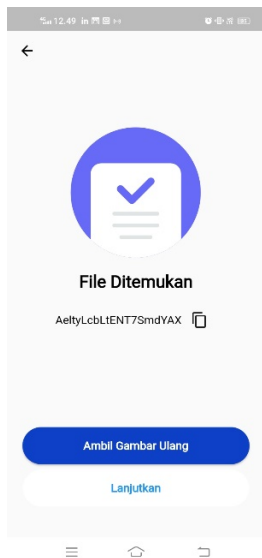
Gambar 14: Halaman *Generate QrCode*



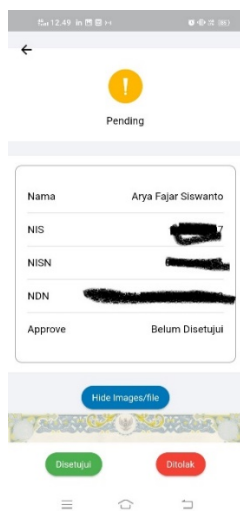
Gambar 12: Pemilihan Gambar



Gambar 15: Halaman *Scan*



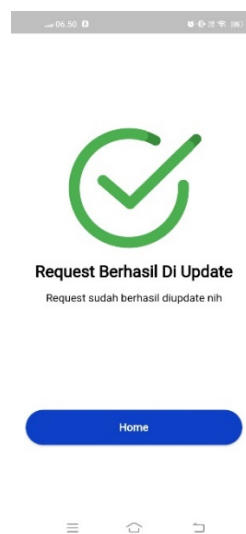
Gambar 16: Halaman *Scan* Ditemukan



Gambar 17: Halaman Detail Permintaan



Gambar 18: Halaman Detail Permintaan 2



Gambar 19: Halaman Validasi *Success*



Gambar 20: Gambar yang di unduh pada halaman *generate* kode Qr.

### Integrasi Pengujian

Integrasi Pengujian dilakukan menggunakan *blackbox* yang berfokus pada fungsionalitas sistem.

Tabel 1 Pengujian *Blackbox*

Fitur	Skenario	Hasil Pengujian
Login	<ul style="list-style-type: none"> <li>- Pengguna masuk dari halaman welcome ke halaman login</li> <li>- Pengguna menginput email atau nim dan password</li> <li>- Pengguna menuju ke halaman Home dan mendapatkan token jika data terdapat didatabase</li> </ul>	Seperti yang diharapkan
Permintaan Validasi	<ul style="list-style-type: none"> <li>- Pengguna Menuju halaman Valdiasi Ijazah</li> <li>- Pengguna diharuskan mengisi semua form yang ada</li> <li>- Pengguna tidak bisa menuju halaman baru jika belum mengisi form atau belum mengupload gambar</li> <li>- Ketika sudah valid dan gambar ijazah pengguna sesuai dengan yang diinput maka pengguna bisa menuju ke halaman Success dan mencetak Kode Qr</li> </ul>	Seperti yang diharapkan

Validasi Permintaan	<ul style="list-style-type: none"> <li>- Pengguna merupakan seorang yang penting dan mempunyai akses untuk memvalidasi</li> <li>- Pengguna menscan Kode Qr yang sudah tergenerate</li> <li>- Pengguna bisa langsung menemukan dan mengakses permintaan sesuai Kode Qr yang berlaku</li> <li>- Pengguna diberikan kebebasan untuk dapat memvalidasi ataupun menolak untuk memvalidasi</li> <li>- Setelah divalidasi maka permintaan akan dianggap selesai</li> </ul>	Seperti yang diharapkan
---------------------	---	-------------------------

### 5. KESIMPULAN

Impelementasi Aplikasi Validasi Serifikat untuk Universitas Esa Unggul berhasil dilakukan dengan baik sesuai dengan *Activity Diagram* yang dibuat. Dimulai dari analisis masalah dan permintaan, studi pustaka, observasi dan wawancara terkait kebutuhan aplikasi. Setelah mendapatkan data yang dibutuhkan dilanjutkan dengan merancang *Activity Diagram*. Lalu merancang *User Interface* di framwork flutter dan membangun database dengan bahasa pemrograman JavaScript dengan framework NodeJs. Implementasi aplikasi validasi sertifikat ini memiliki 3 fitur inti yaitu mengajukan permintaan validasi sertifikat, memvalidasi sertifikat dan mengakses *progress* sertifikat dengan Kode Qr dengan mengamankan data di database menggunakan 3 kombinasi yaitu Base64, AES dan SHA-512.



## 6. Daftar Pustaka

- Asmarajaya, I. K. A., Sanjaya, K. O., Putra, D. M. D. U., Mahendra, G. S., & Hasanah, F. N. U. (2021). Sistem Informasi Keuangan pada Perusahaan Kost Elit dengan Metode Waterfall. *Swabumi*, 9(2), 100–108. <https://doi.org/10.31294/swabumi.v9i2.10970>
- Aziz, M. (2018). Etika Akademis Dalam Pendidikan Islam. *Jurnal Tarbiyah*, 25(1). <https://doi.org/10.30829/tar.v25i1.239>
- Ernawati, S., Wati, R., & Maulana, I. (2021). Penerapan Model Fountain Untuk Pengembangan Aplikasi Text Recognition Dan Text To Speech Berbasis Android Menggunakan Flutter. *Seminar Nasional Aplikasi Sains & Teknologi (SNAST)*, 178–186.
- Firdaus, Yusuf Nur Ikhsan, A. (2022). Aplikasi Validasi Ijazah Menggunakan QR Code Berbasis Web Di Politeknik Negeri Sriwijaya. *Teknik Komputer*, 1(3), 43–50.
- Halim, R. C., & Sugiarto, S. (2018). Penerapan Algoritma AES dalam Perancangan Aplikasi Media Sosial Berbasis Android. *Jurnal ENTER*, 1, 368–379.
- Malabay, M., Herwanto, A., Wahyu, S., & Komul, T. M. P. (2022). Rancangan Album Elektronik Keberkasan Di Era Digital Menuju Good Faculty Governance (Studi Kasus : Fakultas Ilmu Komputer Universitas Esa Unggul). *Infotek : Jurnal Informatika Dan Teknologi*, 5(1), 187–196. <https://doi.org/10.29408/jit.v5i1.4767>