

## PENERAPAN METODE ENKRIPSI BASE64, SHA-512 DAN AES UNTUK MENJAMIN SEBUAH KEABSAHAN IJAZAH (Studi Kasus: Universitas Esa Unggul – Kampus Bekasi)

Arya Fajar Siswanto<sup>1)</sup>, Agus Herwanto<sup>2)</sup>

<sup>1,2)</sup> Teknik Informatika, Universitas Esa Unggul

email: <sup>1)</sup> [aryatgtsfs@gmail.com](mailto:aryatgtsfs@gmail.com), <sup>2)</sup> [agus.herwanto@esaunggul.ac.id](mailto:agus.herwanto@esaunggul.ac.id)

### ABSTRACT

*Security is the most important thing in various aspects of life. Along with the development of technology and information, security is increasingly needed because of the many new crimes that have emerged in society. One of them is diploma forgery, which is a crime that some people are prone to commit. Therefore, it is necessary to validate the certificate to determine whether the document has been legalized or not. Researchers will develop diploma validation applications that focus on validating diplomas that can be accounted for by the party certifying the diploma. This application uses OCR technology which aims to extract data directly from diploma images into text and then compares the results with data entered by the user. To improve data security, this research implements three encryption algorithms, namely Base64, AES, and SHA-512, on servers based on the NodeJs framework. In addition, this application was developed using the waterfall method as a development framework, with the Dart programming language for the Flutter framework and JavaScript for the NodeJs framework.*

**Keywords:** Security, Validate, Diploma

### ABSTRAK

Keamanan merupakan hal paling penting dalam berbagai aspek kehidupan. Seiring berkembangnya teknologi dan informasi, keamanan semakin diperlukan karena banyaknya tindak kejahatan baru yang muncul di masyarakat. Salah satunya adalah pemalsuan ijazah, yang menjadi tindak kejahatan yang rentan dilakukan oleh beberapa orang. Oleh sebab itu, diperlukan adanya validasi ijazah untuk menentukan apakah dokumen tersebut sudah terabsahkan atau belum. Peneliti akan mengembangkan aplikasi validasi ijazah yang berfokus pada pengesahan ijazah yang dapat dipertanggungjawabkan oleh pihak yang mengesahkan ijazah tersebut. Aplikasi ini menggunakan teknologi (OCR) yang bertujuan untuk mengestruk data langsung dari gambar ijazah menjadi teks dan kemudian membandingkan hasilnya dengan data yang dimasukkan oleh pengguna. Untuk meningkatkan keamanan data, penelitian ini mengimplementasikan tiga algoritma enkripsi, yaitu Base64, AES, dan SHA-512, pada server berbasis *framework* NodeJs. Selain itu, aplikasi ini dikembangkan menggunakan metode *waterfall* sebagai kerangka kerja pengembangan, dengan bahasa pemrograman Dart untuk *framework* Flutter dan JavaScript untuk *framework* NodeJs.

**Keywords:** Keamanan, Validasi, Ijazah

## 1. PENDAHULUAN

### 1.1 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. Pandemi COVID-19 merupakan pandemi yang menyebabkan

masyarakat harus menerima perubahan industri 4.0[1]. Perubahan ini meliputi berbagai bidang termasuk dalam pengumpulan berkas dokumen ijazah. Dokumen tersebut sangat rentan diduplikasi oleh pihak yang tidak bertanggung jawab dengan mengubah nama dan informasi yang ada di ijazah tersebut.

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 peneliti ingin menambahkan sebuah wadah memvalidasi ijazah dengan menerapkan teknik kriptografi menggunakan tiga metode enkripsi yaitu Base64, AES dan SHA-512. Selain itu peneliti juga ingin agar mahasiswa yang mempunyai ijazah hanya perlu membuktikan kevalidasian ijazah dengan sebuah Kode Qr yang memudahkan dalam memasukkan bukti pada sebuah dokumentasi.

### 1.2 Identifikasi Masalah

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

### 1.3 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**

### 2.1 Kriptografi

Kriptografi adalah sebuah metode yang digunakan untuk mengamankan data dengan cara 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[2]. Cara kerjanya mengganti dan menggeser blok data yang didasarkan pada kunci. Kunci pada AES dapat memiliki panjang 128-bit, 192-bit dan 256-bit.

### 2.2 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 hitam dan putih.

Kode Qr mampu menyimpan banyak data seperti numerik, alphanumeric, biner, kanji. Selain itu, Kode Qr dapat dibaca dari berbagai sudut dikarenakan terdapat tiga tanda berbentuk persegi di tiga sudut sebagai pembatas kode[3]. Oleh karena itu, kode qr sangat membantu dalam menyimpan kode yang rumit namun tidak terlalu banyak karena akan mengurangi akurasi saat proses membacanya.

### 2.3 OCR

OCR atau Optical Character Recognition 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.

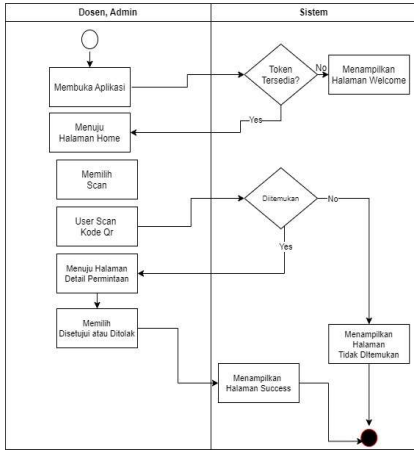
### 2.4 Framework Flutter

Flutter adalah kerangka kerja sumber terbuka (open-source) yang dikembangkan oleh Google. 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 sepertimembuat UI, menambahkan fitur-fitur yang diperlukan dan memperbaiki bug[4].

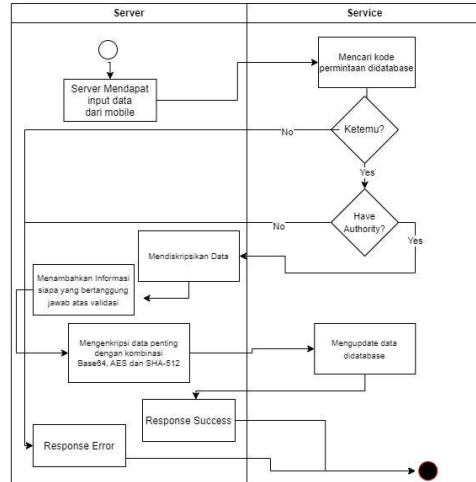
## 3. **METODE PENELITIAN**

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

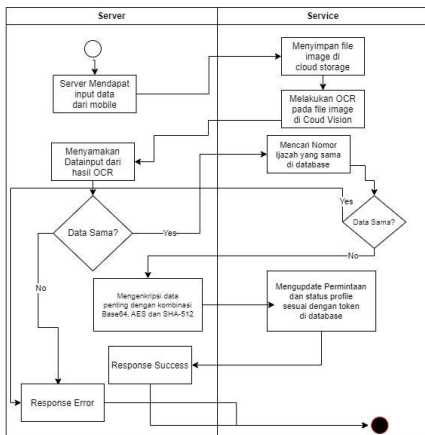




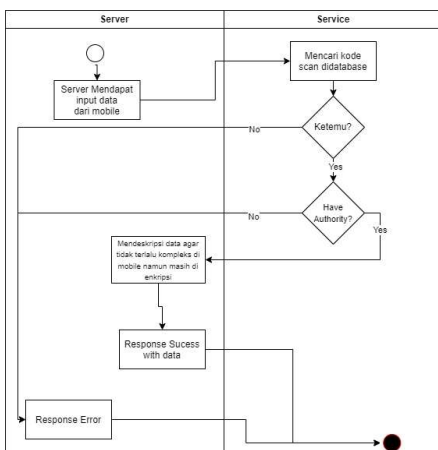
Gambar 4: Activity Validasi Permintaan



Gambar 7: Activity Validasi



Gambar 5: Activity Validasi Sertifikat Backend



Gambar 6: Activity Scan Backend

### 4.3 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.



Esascaan

Makin Mudah Makin Cepat

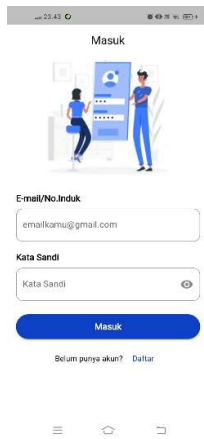
Aplikasi untuk Validasi Ijazah, Iain dan Tanda Tangan QRCode

Daftar

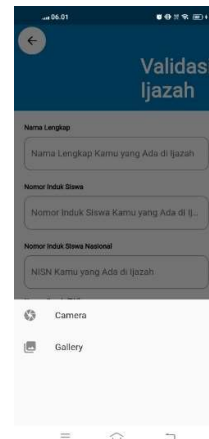
Masuk



Gambar 8: Halaman Welcome



Gambar 9: Halaman Login



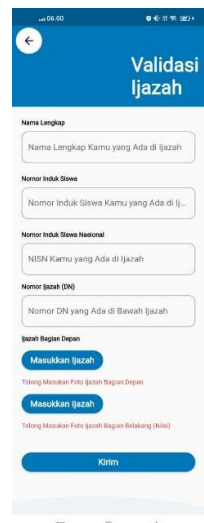
Gambar 12: Pemilihan Gambar



Gambar 10: Halaman Home



Gambar 13: Halaman Success



Gambar 11: Validasi Ijazah



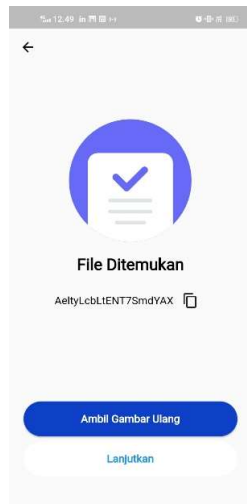
Gambar 14: Halaman Generate QrCode



Gambar 15: Halaman Scan



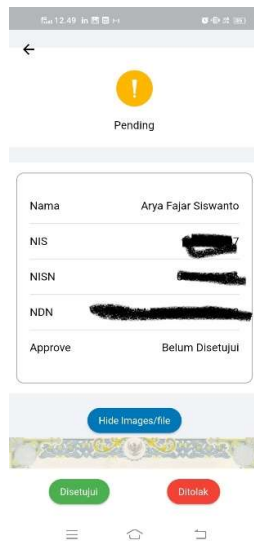
Gambar 18: Halaman Detail Permintaan 2



Gambar 16: Halaman Scan Ditemukan



Gambar 19: Halaman Validasi Success



Gambar 17: Halaman Detail Permintaan



Gambar 20: Gambar yang diunduh pada halaman generate kode Qr

#### 4.4 Integrasi Pengujian

Integrasi Pengujian dilakukan menggunakan blackbox yang berfokus pada fungsionalitas sistem.

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</li> </ul>	Seperti yang diharapkan

	<p>penting dan mempunyai akses untuk memvalidasi</p> <ul style="list-style-type: none"> <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>	
--	---	--

#### 5. SIMPULAN

Implementasi 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. SARAN

Dapat dibangun sebuah model machine learning untuk implementasi OCR berbasis android sehingga tidak harus mengandalkan service Cloud Vision dan menambahkan platform website

7. **REFRENSI JURNAL**

- [1] D. M. Rangkuty, "PROSIDING Konferensi Nasional Universitas Nahdlatul Ulama Indonesia Apakah Penggunaan E-wallet Masa Pandemi Covid-19 Semakin Meningkatkan di Indonesia?," *Pros. Konf. Nas. Univ. Nahdlatul Ulama Indones.*, vol. 01, no. 01, p. 2021, 2021.
- [2] R. C. Halim and S. Sugiarto, "Penerapan Algoritma AES dalam Perancangan Aplikasi Media Sosial Berbasis Android," *J. ENTER*, vol. 1, pp. 368–379, 2018.
- [3] A. Firdaus, Yusuf Nur Ikhsan, "Aplikasi Validasi Ijazah Menggunakan QR Code Berbasis Web Di Politeknik Negeri Sriwijaya," *Tek. Komput.*, vol. 1, no. 3, pp. 43–50, 2022.
- [4] S. Ernawati, R. Wati, and I. Maulana, "Penerapan Model Fountain Untuk Pengembangan Aplikasi Text Recognition Dan Text To Speech Berbasis Android Menggunakan Flutter," *Semin. Nas. Apl. Sains Teknol.*, pp. 178–186, 2021.
- [5] A. Herwanto, S. Wahyu, T. Maria, and P. Komul, "Rancangan Album Elektronik Keberkasan Di Era Digital Menuju Good Faculty Governance ( Studi Kasus : Fakultas Ilmu Komputer Universitas Esa Unggul ) Era digital untuk teknologi informasi terus berkembang , guna menghadapi perkembangan teknologi informasi i," vol. 5, no. 1, pp. 187–196, 2022.
- [6] I. K. A. Asmarajaya, K. O. Sanjaya, D. M. D. U. Putra, G. S. Mahendra, and F. N. U. Hasanah, "Sistem Informasi Keuangan pada Perusahaan Kost Elit dengan Metode Waterfall," *Swabumi*, vol. 9, no. 2, pp. 100–108, 2021, doi: 10.31294/swabumi.v9i2.10970.