

Mobile Platform Biometric Cloud Authentication

Agostinho Marques Ximenes^{1, a}, Sritrusta Sukaridhoto^{2, b}, Amang Sudarsono^{3, c}, Hasan Basri^{4, d}

¹Dept. Informatics Engineering, Insitituto Superior Cristal, Doad Balide, Dili, Timor Leste

^{2,3}Program Studi Teknik Informatika dan Komputer, Politeknik Elektronika Negeri Surabaya,
Jl. Raya ITS, Surabaya, Jawa Timur, Indonesia

⁴Program Studi Manajemen Informatika, Politeknik Negeri Fakfak,
Jl. Imam Bonjol Atas, Air-Merah, Wagon, Fakfak, Papua Barat, Indonesia

^aagusmarques1@gmail.com,

^bdphoto@pens.ac.id

^camang@pens.ac.id

^dhasan@polinef.id



Abstract—Based on the Indonesian Central of Statistics the level of poverty people in September 2018 was 25.95 million, based on data, the government allocation care funds the reduce poverty people, the fund is given through the bank. However, the bank cannot allocation funds because the cost for build infrastructure is expensive, such as making an ATM. about that, the banks need to find a new solution to allocation care fund to the poverty people. In this paper, a mobile platform biometric cloud authentication is one of platform used for the online payment transaction at merchants. The implementation of the biometric face recognized (face data encrypt and decrypt used algorithm AES 256 bit) and QR Code to secure online payment merchant base on mobile cloud authentication, that play role in data communications security. The test results on this mobile application show that scanning a QR Code and biometric face recognized can be implemented at an online merchant transaction with an accuracy of 95% and takes 53, 21 seconds in transactions.

Keywords—*Biometrics; Cloud; Cryptography; QR Code.*

Abstrak—Berdasarkan data Pusat Statistik Indonesia, tingkat kemiskinan pada bulan September 2018 adalah 25,95 juta, berdasar data tingkat kemiskinan masyarakat tersebut pemeritnah menyalurkan dana bantuan mengatasi tingkat kemiskinan masyarakat melalui Bank. Namun, Bank tidak dapat mengalokasikan dana karena biaya untuk membangun infrastruktur mahal, seperti membuat ATM. Berbagai kendala tersebut, Bank perlu menemukan solusi baru agar dapat mengalokasikan dana kepada masyarakat dengan biaya yang murah, Mobile Platform Biometric Cloud Authentication adalah salah satu solusi. Dalam penelitian ini, eksperimen yang dilakukan melakukan autentikasi dengan QR Code Scan dan *face recognize* (data *face* dienkripsi dan didekripsi dengan kriptografi algoritma AES 256 bit). Konsentrasi penelitian ini terletak pada eksperimen terhadap komunikasi keamanan data transaksi *payment merchant onlie* dengan *QR Code scan* dan *Face recognize* yang berbasis mobile android dan serta spesifikasi android versi 23. Hasil pengujian pada aplikasi Mobile ini menunjukkan bahwa QR Code scan dan *face recognize* dapat

diimplementasikan pada transaksi *payment merchantonline* dengan akurasi 95% dan membutuhkan 53, 21 detik per transaksi.

Kata Kunci—*Biometrik; Server Cloud; Kriptografi; QR Code.*

I. Pendahuluan

Berdasarkan data Badan Pusat Statistika Indonesia tingkat kemiskinan masyarakat pada bulan September tahun 2018 sebanyak 25.95 juta orang [1], berdasarkan data tersebut maka pemerintah melakukan penangulangan tingkat kemiskinan masyarkat dengan memberikan dana kesejahteraan kepada masyarkat miskin, bantuan tersebut disalurkan melalui Bank. Namun bank memiliki kendala untuk mencairkan dana karena biaya pembangunan infrastruktur dan administrasi yang mahal seperti pembuatan ATM.

Perkembangan teknologi dan ketergantungan manusia terhadap teknologi, dan serta teknologi sudah merambah ke berbagai bidang baik itu industri, manufaktur, pendidikan, pemerintah, bisnis, perbankan, dan serta kehidupan sehari-hari manusia [2]-[4].

Mobile sebagai salah satu pelayanan yang sangat berkembang saat ini, karena dengan mobile sangat membantu dan mempermudah bagi pengguna bisa mengakses data dan informasi dimana saja tanpa dibatasi oleh media, ruang, waktu untuk mengaskes data dan informasi yang diinginkan dan serta pengiriman data lebih cepat dan murah. Namun sisi keamanan sebagai salah satu kendala sering dihadapi baik berupa pencurian data,

pengecatan data, kecurangan, dan pengaksesan data yang tidak sah [5], [6].

Sistem yang digunakan dalam keamanan saat ini terdiri dari sistem keamanan data dengan menggunakan teknik keamanan tradisional dengan kriptografi dan teknik keamanan modern dengan biometrik dan QR Code [7]. Kriptografi merupakan teknik penyamaran teks asli ke teks acak dengan menggunakan kunci, biometrik menggunakan karakteristik manusia berupa sidik jari, retina, wajah, telapak tangan, DNA, dan telapak kaki untuk melakukan autentikasi [8].

Teknik keamanan data dan transaksi menggunakan teknik keamanan kriptografi dan biometrik masih memiliki kelemahan, dengan menggunakan teknik kriptografi memiliki kelemahan pengecatan data, manipulasi data, perusakan data, dan serta penyebaran data ke pihak lain. Teknik keamanan modern dengan biometrik masih memiliki kelemahan atas pemalsuan karakteristik biometrik.

Dari permasalahan tersebut yang akan dibahas sebagai berikut: (1) Memberikan solusi untuk mencairkan dana masyarakat dengan membangun aplikasi mobile transaksi, (2) Melakukan penyamaran data biometrik agar data biometrik tidak mudah dipalsukan. (3) Melakukan penggabungan sistem QR Code, biometrik (*face*) dan kriptografi (AES 256 bit) agar bisa menghasilkan tingkat autentikasi yang lebih kuat, handal dan aman, (4) Akurasi pada tingkat autentikasi biometrik untuk transaksi, dan (5) Mengukur berapa lama waktu yang dibutuhkan untuk melakukan transaksi.

Berbagai permasalahan yang telah diidentifikasi maka peneliti mengajukan suatu pendekatan penyaluran dana masyarakat kepada Bank dengan biaya pembangunan fasilitas yang murah, dan serta tingkat keamanan transaksi data yang aman, handal, dan kuat dengan membangun sebuah platform mobile dengan nama *Mobile Platform Biometric Cloud Authentication*.

II. Metode Penelitian

A. Biometric Face Recognize

Biometrik merupakan suatu teknik untuk mengidentifikasi seseorang dengan menggunakan karakteristik salah satu bagian dari tubuh manusia [9], [10]. Salah satu bagian tubuh manusia yang digunakan

pada biometrik ini adalah *face* atau wajah. Teknik pengenalan seseorang menggunakan *face recognizes* atau pengenalan wajah pada saat ini banyak digunakan dalam sistem keamanan suatu perangkat. Salah satu sistem keamanan menggunakan *face recognizes* untuk mengunci dan membuka sebuah pintu atau perangkat mobile [5].



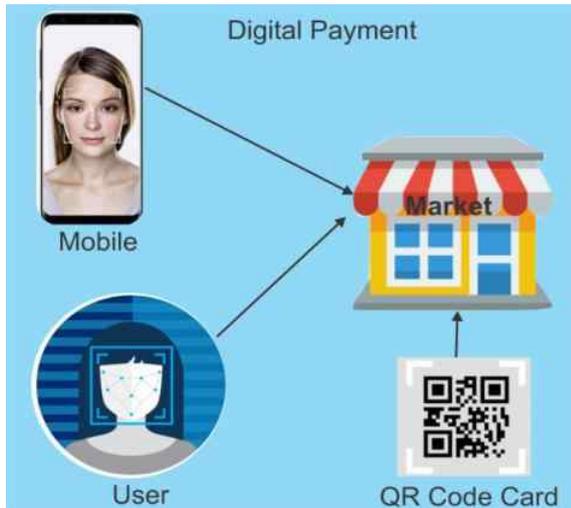
Gambar1. Biometric Face Recognize

Pada gambar 1 menjelaskan bahwa data wajah dari seseorang dapat disimpan dalam sebuah database dengan merubah data wajah menjadi sebuah karakter. Pengenalan pola posisi wajah dengan membuat persegi pada wajah untuk menentukan titik-titik pola wajah dan menentukan posisi wajah dengan mengambil nilai [9]. Autentikasi menggunakan pengenalan wajah atau *face recognize* terdapat 2 proses utama yaitu melakukan proses identifikasi wajah dengan melakukan penentuan posisi wajah, menentukan atribut yang diambil untuk melakukan training untuk mendeteksi wajah dan proses *face recognize* atau pengenalan wajah dengan melakukan pencocokan wajah antara data wajah yang telah di simpan di database dengan pengambilan potot wajah baru [9], [10].

B. Android Mobile APPS untuk Digital Payment

Android Mobile apps atau aplikasi mobile android adalah aplikasi yang dibuat untuk smartphone, dapat diinstal dan dioperasikan di platform smartphone android. Android mobile apps berjalan pada java programming. Digital payment merupakan konsep transaksi yang berbasis digital. Jadi *android mobile APPS for digital payment* adalah sebuah aplikasi mobile android yang memanfaatkan fitur-fitur yang terdapat

pada smartphome mobile untuk melakukan transaksi pembayar, yang terdapat pada gambar 2.



Gambar 2. Android Mobile APPS for digital payment

a. QR Code

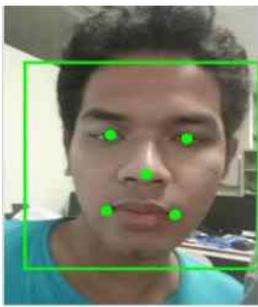
QR Code (*Quick Response Code*) adalah dua dimensi yang dapat menyimpan data. QR code digunakan pertama kali di dunia otomotif untuk melakukan pelacakan bagian dari rangkaian kendaraan. Semakin berkembangnya penggunaan QR Code banyak di gunakan untuk menyebarkan alamat website. Nomor kontak, alamat email, nomor telepon, bahkan untuk pembayaran. Maka kehadiran sistem pembayara yang pada saat ini dan yang akan teknologi terus berkembang, menggunakan sistem pembayaran dengan salah satu sistem pembayaran teknologi QR Code (*Quick Response Code*) atau QR Paymnetsebagai solusi untuk mengatasi kebutuhan manusia atas keamanan data transaksi yang aman dan efesien [11]. ilustrasiQR Code pada gambar 3.



Gambar 3. QR Code

b. Face API Azure

Azure Face API adalah sebuah service algoritma cognitive untuk deteksi, pengenalan, dan menganalisa wajah manusia dalam gambar. Algoritma cognitive memiliki kemampuan untuk proses informasi yang ada wajah manusia, dan informasi tersebut bisa di implementasikan kedalam berbagai sistem keamanan IU/UNIX pada mobile dan robot.Service cognitive Azure merupakan services kecerdasan buatan Microsoft berbasis cloud yang dapat digunakan pengembangan aplikasi berbasis *artificial intelegent* [9]. Pada *Face API* terdapat 2 proses, yaitu (1) *face detection API* untuk mendeteksi wajah manusia dalam gambar dan membuat koordinat lokasi persegi pada wajah. Setelah wajah dideksi ekstraksi fitur yang terkait dengan atribut wajah seperti pose, pose kepala, jenis kelamin, umur, emosi, rambut wajah, dan kacamata seperti pada gambar 4. (2) *Face verification API* untuk melakukan autentikasi dengan data wajah baru yang di ambil dengan kamera mobile dan melakukan deteksi wajah setelah wajah di deteksi maka data di lakukan pencocokan data wajah yang yang ada di database wajah. seperti pada gambar 5.



Gambar 4. Face Detect



Gambar 5. Face verify

Pada gambar 4 merupakan proses deteksi wajah dan sebelah kanan gambar 5 sebagai proses verifikasi wajah

c. Merchant

Merchant adalah penjual barang atau jasa yang memiliki bentuk usaha (*physical store*) maupun *online store* yang bekerjasama dengan Bank dalam penyediaan layanan penerimaan pembayaran via e-money bank yang bersangkutan [7]. Merchant dibagi menjadi dua yaitu merchant perorangan dan merchant berbadan hukum. Merchant perorangan adalah merchant milik perorangan tanpa berdasarkan pada tata cara dan ketentuan pendirian usaha berbadan hukum. Sedangkan merchant berbadan hukum adalah merchant yang didirikan berdasarkan pada tata cara dan ketentuan pendirian usaha berbadan hukum yang berlaku. Setelah perorangan atau badan usaha mendaftar sebagai merchant, maka selanjutnya mereka akan memperoleh ID merchant. Ilustrasi merchant pada gambar 6.



Gambar 6. Merchant Online

d. Mobile Cloud Computing

Mobile cloud computing merupakan salah satu infrastruktur yang melakukan penyimpanan data dan proses yang dilakukan di luar dari pada perangkat mobile [12], [13], perangkat mobile memindahkan data komputasi dan melakukan penyimpanan data bukan langsung pada perangkat mobile melainkan

penyimpanan data di cloud. Fitur yang sangat penting daripada platform mobile cloud terletak kolaborasi fungsionalitas antara platform mobile dengan cloud, dan melakukan akses melalui nirkabel yang berbasis pada web base atau client pada mobile platform [14]-[16].

C. Metode penelitian

Metode penelitian yang dilakukan menggunakan metode penelitian kuantitatif dengan menganalisa tingkat akurasi verifikasi wajah dan QR Code dan waktu yang di perlukan untuk melakukan transaksi .

D. Bahan penelitian

Pada penelitian ini menggunakan beberapa software pendukung sebagai berikut:

Tabel 1: bahan penelitian

spec	Mobile	PC Server
type	Samsung S8	Cloud server
proc	Exynos 9 octa 8895	Intel Xeon 4 Core Xeon
Ram	6GB	16 GB
OS	Android	Linux Debian
Camera	8px	-
Database	-	MongoDB
connect	4G	1Gbs/100Mbs

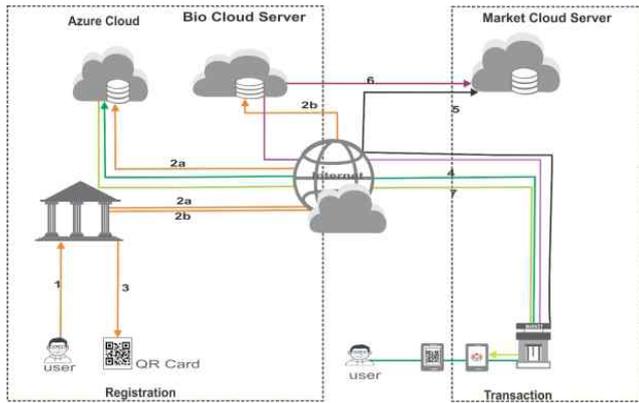
E. Prosedur pengujian

Mobile Platform Biometric Cloud Authentication ada 2 bagian utama proses yaitu, (1) proses registrasi yang terdiri dari enrolment, *store data to the cloud*, dan *create QR Code*. (2) pada proses transaksi terdiri dari proses *scan QR Code* dan *face verification*, *store transaction data*, *check balance*, dan *transaction permission*.

III. Hasil dan Pembahasan

Pada tahap ini, melakukan pengujian terhadap implementasi dari *desain system Mobile Platform Biometric Cloud Authentication(MPBCA) architecture* yang memiliki 2 proses utama yaitu, (1) proses registrasi (*enrolment, store data to cloud, create QR Code*), dan (2) transaksi (*scan QR Code+ Face recognize, store data to cloud market, check balance, dan transaction permission*).

A. Arsitektur Mobile Platform



Gambar 7. Arsitektur Mobile Platform

Desain sistem arsitektur Mobile Platform terdapat 2 proses utama yaitu;

a. Tahap Registrasi

1. *Enrolment*, pada tahap pendaftaran melakukan pengisian nama, kunci, alamat tempat tinggal, nomor infok penduduk (KTP), tempat tanggal lahir, jenis kelamin, saldo, pengambilan potot biometrik wajah.
2. *store data*, menyimpan data wajah yang telah dienkrpsi disimpang ke database cloud server yang dibuat oleh peneliti.
3. *Create CQ Code*, sebagai kartu QR Code berupah logi ke aplikasi.

b. Tahap Transaksi

1. *Scan QR Code and Face recognize*, tahap ini melakukan scan kartu QR code pengguna dan melakukan pengenalan wajah.
2. *Store transaction data*, tahap melakukan penyimpanan data transaksi di cloud server *market*.
3. *Check balance*, pada tahap ini melakukan pengecekan saldo terhadap jumlah bayaran yang akan di bayar.
4. *Transaction permission*, melakukan proses transaksi setelah melakukan cek balance saldo, jika saldo cukup maka proses transaksi berhasil, jika tidak maka proses transaksi gagal.

Pada proses registrasi dan transaksi pada aplikasi tersebut dipaparkan dalam arstiketerur *mobile platform biomerik authentication* pada gambar 6.

B. Pada proses menu registrasi terdapat 3 proses utama yaitu:

a. Proses ujicoba Menu Enrolment

Proses menu enrolment merupakan tahap registrasi yang terdiri dari 4 proses yaitu, (1) input user-id, (2) megambil gambar wajah, (3) deteksi wajah, dan (4) proses untuk simpan ke database. Ilustrasi terdapat pada gambar 8.



Gambar 7. Ujicoba Proses Registrasi

Pada proses *enrolment* gambar 7, bagian nomor (1) menu proses *user-id* terdapat beberapa atribut yang digunakan yaitu, (a) *name* berisi nama, (b) *private key* sebagai masukan untuk mengunci gambar *face person* kunci menggunakan algoritma AES 256 bit, (c) *address* untuk masukan alamat *user*, (d) *nationa-id* sebagai input nomor KTP, (e) *birth info* input tempat dan tanggal lahir, (f) *gender* untuk input jenis kelamin, dan (f) *balance* digunakan untuk *input* saldo user simapng di bank.

Pada proses *enrolment* gambar 7, bagian nomor (2) tedapat 2 proses yaitu (a) dengan *button* take a photo digunakan untuk mengambil poto wajah secara *real-time* atau langsung dengan kamera belakang dan (b) dengan *button* from gallery digunakan untuk melakukan *input* gambar wajah dari komputer atau bukan dengan kamera belakang mobile secara langsung.

Pada proses *enrolment* gambar 7, bagian nomor (3) merupakan proses pengambilan poto wajah dengan kamera belakang secara *real-time* atau langsung.

Pada proses *enrolment* gambar 7, bagian nomor (4) merupakan hasil proses deteksi wajah pada gambar potoh yang di ambil.

Pada proses *enrolment* gambar 7, bagian nomor (5) merupakan data *face person* yang tersimpang di dabase *face bio*.

b. Proses ujicoba Simpan Data user Cloud Server

#	users						
1	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce876761c02104209304de3</td> <td>[] 4 elements</td> <td>"DnAIMKcP3PVgIm6eoeGQwBgJm9PKZ</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce876761c02104209304de3	[] 4 elements	"DnAIMKcP3PVgIm6eoeGQwBgJm9PKZ
_id ObjectId	personFaces Array	name String					
Sce876761c02104209304de3	[] 4 elements	"DnAIMKcP3PVgIm6eoeGQwBgJm9PKZ					
2	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce694a11c02104209304de4</td> <td>[] 1 elements</td> <td>"DnAIM28yNXZHTH10yK-BBoD7K1C16</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce694a11c02104209304de4	[] 1 elements	"DnAIM28yNXZHTH10yK-BBoD7K1C16
_id ObjectId	personFaces Array	name String					
Sce694a11c02104209304de4	[] 1 elements	"DnAIM28yNXZHTH10yK-BBoD7K1C16					
3	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce695af1c02104209304de5</td> <td>[] 2 elements</td> <td>"DnAIMa5MAQRhuuU-AN3o9LvaPInB_</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce695af1c02104209304de5	[] 2 elements	"DnAIMa5MAQRhuuU-AN3o9LvaPInB_
_id ObjectId	personFaces Array	name String					
Sce695af1c02104209304de5	[] 2 elements	"DnAIMa5MAQRhuuU-AN3o9LvaPInB_					
4	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce696661c02104209304de6</td> <td>[] 1 elements</td> <td>"DnAIMx6IRD73kHC33W4TKXJ5FMly</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce696661c02104209304de6	[] 1 elements	"DnAIMx6IRD73kHC33W4TKXJ5FMly
_id ObjectId	personFaces Array	name String					
Sce696661c02104209304de6	[] 1 elements	"DnAIMx6IRD73kHC33W4TKXJ5FMly					
5	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce697831c02104209304de7</td> <td>[] 1 elements</td> <td>"DnAIMz311EqokkyIweIm3-Cb6PeWb</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce697831c02104209304de7	[] 1 elements	"DnAIMz311EqokkyIweIm3-Cb6PeWb
_id ObjectId	personFaces Array	name String					
Sce697831c02104209304de7	[] 1 elements	"DnAIMz311EqokkyIweIm3-Cb6PeWb					
6	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce698871c02104209304de8</td> <td>[] 1 elements</td> <td>"DnAIM6NLoITsh--EhJ28DHUta139_</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce698871c02104209304de8	[] 1 elements	"DnAIM6NLoITsh--EhJ28DHUta139_
_id ObjectId	personFaces Array	name String					
Sce698871c02104209304de8	[] 1 elements	"DnAIM6NLoITsh--EhJ28DHUta139_					
7	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce698831c02104209304de9</td> <td>[] 1 elements</td> <td>"DnAIM2xqeXDNix1brBjxfkr1zsdUX</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce698831c02104209304de9	[] 1 elements	"DnAIM2xqeXDNix1brBjxfkr1zsdUX
_id ObjectId	personFaces Array	name String					
Sce698831c02104209304de9	[] 1 elements	"DnAIM2xqeXDNix1brBjxfkr1zsdUX					
8	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sce69a531c02104209304dea</td> <td>[] 1 elements</td> <td>"DnAIMxvXT3yI2n5L81_Cj067kt7j2</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sce69a531c02104209304dea	[] 1 elements	"DnAIMxvXT3yI2n5L81_Cj067kt7j2
_id ObjectId	personFaces Array	name String					
Sce69a531c02104209304dea	[] 1 elements	"DnAIMxvXT3yI2n5L81_Cj067kt7j2					
9	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>S082167d1c02104209304deb</td> <td>[] 1 elements</td> <td>"DnAIMdEMhBONQCLJIm16-W0u8kFCV</td> </tr> </table>	_id ObjectId	personFaces Array	name String	S082167d1c02104209304deb	[] 1 elements	"DnAIMdEMhBONQCLJIm16-W0u8kFCV
_id ObjectId	personFaces Array	name String					
S082167d1c02104209304deb	[] 1 elements	"DnAIMdEMhBONQCLJIm16-W0u8kFCV					
10	<table border="1"> <tr> <th>_id ObjectId</th> <th>personFaces Array</th> <th>name String</th> </tr> <tr> <td>Sd121d691c02104209304dec</td> <td>[] 1 elements</td> <td>"DnAIMp81E2x6WU-4Q8ftmBmrIF-s</td> </tr> </table>	_id ObjectId	personFaces Array	name String	Sd121d691c02104209304dec	[] 1 elements	"DnAIMp81E2x6WU-4Q8ftmBmrIF-s
_id ObjectId	personFaces Array	name String					
Sd121d691c02104209304dec	[] 1 elements	"DnAIMp81E2x6WU-4Q8ftmBmrIF-s					

Gambar 8. Database Cloud Bio

Pada implementasi store database bio ke cloud server yang di bangun oleh peneliti dengan alamat jaringan server cloud, SLLpada gambar 4.3, database yang di bangun menggunakan mongoDB, database yang dibangun dengan nama *bio* dan tabel dengan nama *users* dengan memiliki kolom 12 yang terdiri dari, (1) *id* object bersih *id face*, (2) *person-faces* berisi jumlah potoh yang di di simpan di dabase, (3) *name* berisi nama daripada *user*, (4) *person-id* id dari *person*, (5) *private key* berisi kunci algoritma AES 256 bit untuk enkripsi *face*. (6) *qurl* merupakan url dari jaringan, (7) *balance* merupakan saldo user yang ada di bank, (8) *gender* berisi jenis kelamin dari *user*, (9) alamat sebagai alamat tempat tinggal dari *user*, (10) *nid* adalah id ktp dari *user*, (11) *ttl* merupakan sebangai tempat tanggal lahir, dan (12) *V* merupakan jumlah dari potoh *face*.

c. Proses ujicoba create QR Code User

Proses pembuatan *QR Code* sebagai kartu tanda pengenal bagi *user*. Ilustrasai *QR Code* user pada gambar 9.



Gambar 9. Create QR

Pada proses pembuatan *QR Code* user pada gambar 9 dengan menggunakan gambar wajah *user* dan di enkripsi gambar wajah agar tidak mudah di baca code *QR Code*, *QR Code* sebagai kartu tanda pengenal *user*.

C. Proses Ujicoba Menu Transaksi

Pada proses menu transaksi ada 7 proses yaitu, (1) *scan QR Code*, (2) *face detection*, (3) *face verification*, (4) store transaction data, (5) *input amount to pay*(*check balance*), dan (6) *transaction permission*.

a. Proses Menu ujicoba Scan QR Code

Implementasi proses menu *scan QR Code* dan *face verification* merupakan proses autentikasi untuk

melakukan proses transaksi. Dalam uji coba yang terdapat pada gambar 10.



Gambar 10. Scan QR Code

Hasil ujicoba scan QR Code pada gambar 10 tahap proses scan QR code ada 2 tahap yaitu, (1) masukan jumlah uang akan di bayar atas pembelian barang ke dalam teks *input*, (2) menempelkan kartu QR pada kamera belakang mobile samapai bentuk kartu QR Code semua tampil di segi empat pada menu scan QR Code. Dan proses scan akanberlanjut ke proses selanjutnya.

b. Proses Ujicoba Face Detection Dan Face Verification



(1) Proses take a picture (2) Proses face detection

Gambar 11. Ujicoba Face Detection&Verification

Hasil ujicoba proses *face detection* pada tabel 11 memiliki 2 tahap proses *face detection*, yaitu (1) mengambil potret dengan kamera depan pas pada kotak segi empat pada mobile apps dan (2) tekan *button detect* untuk melakukan dekripsi face user dan melakukan matching *face* jika ada di database maka memberikan hasil detect seperti pada gambar 4.5 bagian kanan dengan proses menu *face detection*.

c. Proses ujicoba verifikasi

Pada proses ini merupakan langkah untuk melakukan verifikasi *face* dan transaksi. Ujicoba pada ilustrasi gambar 12.



Gambar 12. Ujicoba Proses Verifikasi

Pada bagian proses face verification pada gambar 12 merupakan proses permission transaction, terdapat 2 tahap proses yaitu (1) setelah face sudah di deteksi dan melakukan matching antara face baru yang di ambil dengan kamera depan dengan face yang ada di database cloud server untuk melakukan matching maka autor mendapat konfidensial, (2) proses verifikasi untuk melakukan permission transaction, jika saldo balance dengan jumlah transaksi maka proses transaksi sukses dan sebaliknya.

d. Ujicoba Storage Transaction Data

Storage transaction data merupakan proses untuk menyimpan data transaksi market di database cloud server market. Ilustrasi Ujicoba penyimpanan data transaksi pada gambar 13.

#	transactions
1	{ "_id": "5c693275c86a8140bc9fa2c0", "transactionId": "DNA2MCLNHRKPeqenIsot8u770u9s3", "userId": "3e0f1559-8b7d-4288-b664-e093a8", "merchantId": "merchantId" }
2	{ "_id": "5c6944ccc86a8140bc9fa2c1", "transactionId": "DNA2MNBHvjP5G1DQuLrVj3hs-6P-Y", "userId": "bb079625-fdea-46f3-84e8-7b765d", "merchantId": "merchantId" }
3	{ "_id": "5c697728c86a8140bc9fa2c2", "transactionId": "DNA2Mh3Jq2Jwv1j1a1FXyTE0aQ878V", "userId": "0a7aabc5-37a3-48cb-b65c-918a5d", "merchantId": "merchantId" }
4	{ "_id": "5c69320bc86a8140bc9fa2c3", "transactionId": "DNA2MhC40b5x59Tra05Pb6_cwcyer", "userId": "0a7aabc5-37a3-48cb-b65c-918a5d", "merchantId": "merchantId" }
5	{ "_id": "5c695588c86a8140bc9fa2c4", "transactionId": "DNA2MhCLtP8U5Lr_wK2kP51FOLr2BS", "userId": "9a579640-f76e-4d8e-a88d-b93794", "merchantId": "merchantId" }
6	{ "_id": "5c695f6cc86a8140bc9fa2c5", "transactionId": "DNA2MhRU2T5Cq0G6u2Vkhvee2F6", "userId": "73a58967-ea9f-463b-8a8b-3cef36", "merchantId": "merchantId" }
7	{ "_id": "5c69784cc86a8140bc9fa2c6", "transactionId": "DNA2MhA0y8p8tvd1U6vG1Yd-Q_X", "userId": "b7ea76a5-8949-4109-969f-c34a81", "merchantId": "merchantId" }
8	{ "_id": "5c698012c86a8140bc9fa2c7", "transactionId": "DNA2MhUwEj_34F0Qq53m83-mR12G", "userId": "59f29909-1a33-4658-b085-e16514", "merchantId": "merchantId" }
9	{ "_id": "5c6990f8c86a8140bc9fa2c8", "transactionId": "DNA2MhK4TaTKLzFLt8-w3ccQ0q8", "userId": "b43c663a-389c-4d6c-b93c-d8a458", "merchantId": "merchantId" }
10	{ "_id": "5c699e3cc86a8140bc9fa2c9", "transactionId": "DNA2MhKer0PvF58I8F2FkAstvYj_A", "userId": "f4586663-b722-4954-86ee-64ceff", "merchantId": "merchantId" }

Gambar 13. Ujicoba Database Transaction Market

Pada ujicoba *store data transaction* pada database market di cloud server dengan alamat jaringan server cloud SSL gambar 13 dengan nama database *market*, *table transaction* dan terdapat 7 kolom yang terdiri dari (1) id-object isi data face, (2) transaction-id berisi data transaksi, (3) userid merupakan id dari *user*, (4) merchantid berisi data tempat transaksi, (5) *balancebefore* berisi saldo user sebelum dikurang dengan transaksi, (6) *transaction amount* berisi total transaksi, (7) *balance after* berisi sisah saldo di bank.

e. Ujicoba Check Balance Transaction

Pada Tahap Ini Melakukan Balance Check Transaksi, Ilustrasi Transaksi Pada Gambar 14.



Gambar 14. Uji Coba Check Balance

Pada gambar 14 merupakan ujicoba dari *balance transaction*, dalam melakukan ujicoba terhadap *balance transaciton* menggunakan 2 kondisi yaitu, kondisi (1) *transaction success* jika melakukan *check balance* saldo bank dengan jumlah barang yang dibeli dimana saldo bank lebih besar atau sama dengan jumlah transaksi, kondisi (2) *transaction fail atau current account not enough to pay*, jika melakukan *check balance* saldo bank dengan jumlah barang yang dibeli dimana saldo bank lebih kecil daripada jumlah transaksi yang akan dibayar.

f. Transaction permission

Ada scenario ini melakukan *face detects* dan *face error*. Ulustrasi pada gambar 15.

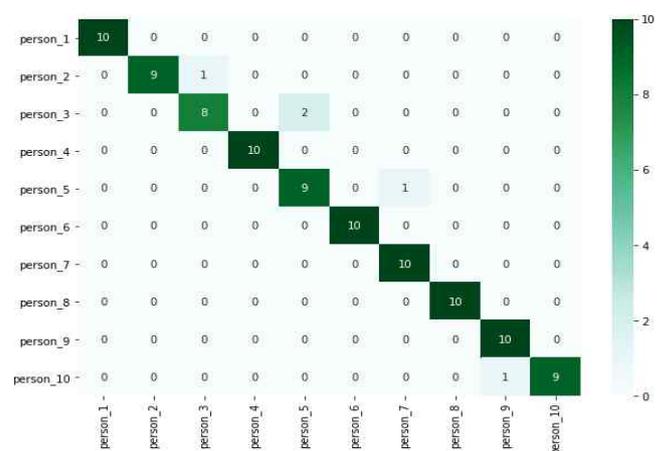


Gambar 15. Face Detection dan Face Error

Pada skenario pada gambar 15 merupakan hasil dari face detect dan face error. Pada gamabr face A ujicoba face detect karena face dan QR code sama orang dan face terdaftr pada database face di server cloud, sedangkan face error pada gamgar B sebaliknya.

D. Ujicoba Akurasi Proses Face Recognize

Pada hasil ujicoba permission acces transaction terhadap 10 orang untuk menganalisa tingkat akurasi kerbhasilan mobile apss melakukan transaction success dengan face recognize. Analisa ujicoba akurasi pada gambar 16.pada suatu aplikasi dikatakan memiliki akurasi yang tinggi jika dapat memberikan hasil output dari sebuah input dengan benar. Pada penelitian ini, tingkat akurasi diukur berdasarkan tingkat keberhasilan dalam melakukan kembali verifikasi wajah pada orang yang sama menghasilkan nilai *true* dan nilai *falsa* pada wajah yang berbeda.

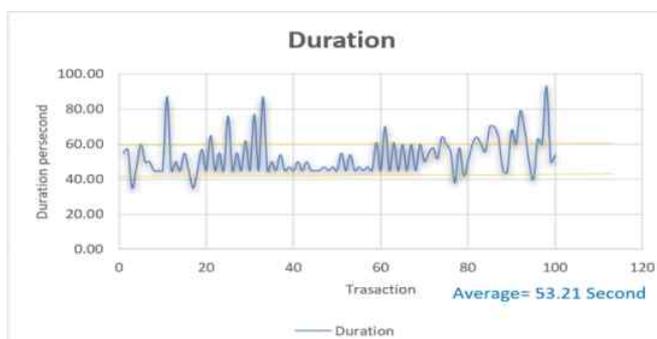


Gamabr 16. Grafik Akurasi Transction Permission

Pada gambar 16 grafik data *transaction permission* terhadap 10 orang sampel ujicoba permission transection menggunakan beda face orang antar 1 samapi 2 orang berbeda success memberikan hasil bahwa fail *transaction*, sehingga hasil dari ujicoba memenuhi standar akurasi *output* sesuai dengan *input*. Dari hasil ujicoba dengan akurasi sebesar 95% t permission transaction.

E. Ujicoba Time Speed Proses Transaksi

Proses ujicoba *time speed* untuk mengukur lama waktu dalam satu waktu melakukan proses autentikasi *face verification*. Ilustrasi ujicoba time speed pada gambar 17.



Gambar 17. Grafik Time Speed Transaction

Dari hasil analisis pada time speed pada gambar 17, menunjukan bahwa waktu yang dibutuhkan untuk melakukan transaction permission hanya membutuhkan waktu rata-rata 53.21 second untuk melakukan sekali transaksi, dengan data transaksi sebanyak 100 kali.

IV. Kesimpulan

Mobile Platform Biometric Cloud Authentication adalah mobile apps autentikasi dengan biometric untuk melakukan *permission transaction*. *Permission transaction* menggunakan beberapa data berupa seperti kartu *QR Code* dan *Face recognize* atau *verification*. Biometrik autentikasi adalah autentikasi dengan menggunakan salah satu bagian tubuh manusia seperti wajah, retina, sidik jari, suara, dan lainnya.

Konsep *Mobile Platform Biometric Cloud Authentication* yang diterapkan adalah metode algoritma AES 256bit digunakan untuk enkripsi dan dekripsi biometrik *face*. Agar untuk mencega pemalsuan data biometrik *face*.

Permission transaction yang digunakan adalah kartu *QR Code* dan *face authentication*, data *face* disimpan di cloud server sehingga mudah melakuakn kontrol dan manajemen. *Mobile apps authentication* dibangun menggunakan sistem operasi android minimal API Level 22 lollipop.

Dari keseluruhan dari penelitian atas tesis ini disimpulkan bahwa :

- 1) Terdapat 2 proses utama dalam implentasi yaitu, registrasai dan transaksi.
- 2) Mobile transaction permission di implementasikan untuk transaksi *merchant* dan berjalan secara *online access*.
- 3) *Authentication permission transaction* menggunakan 2 kali autentikasi, yaitu (1) dengan *QR Code* (2) *face verification*.
- 4) Biometrik *face authentication* enkripsi dan dekripsi dengan algoritma AES 256 bit.

aplikasi yang dibangun dengan mobile android dengan tingkat akurasi permission *transaction* 95% dan time speed 53,21 second per transaksi.

Daftar Pustaka

- [1] Badan Pusat Statistik Indonesia, "Profil Kemiskinan di Indonesia September 2017," *BPS (Badan Pusat Statistics)*, 2018, vol. 01, Jakarta, pp. 1–12.
- [2] I.M.Alsaadi, "Physiological Biometric Authentication Systems , Advantages , Disadvantages And Future Development : A Review," 2015, *Int. J. Sci. Technol. Res.*, vol. 4, no. 12, pp. 285–289.
- [3] B. Ammour, T. Bouden, and S. Amira-Biad, "Multimodal biometric identification system based on the face and iris," 2017, *5th Int. Conf. Electr. Eng. - Boumerdes, ICEE-B 2017*, vol. 2017-Janua, pp. 1–17.
- [4] D. Chen, X. Cao, F. Wen, and J. Sun, "Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification," 2013, *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 3025–3032.
- [5] D. Chen, X. Cao, L. Wang, F. Wen, and J. Sun, "Eccv_2012_Bayesian.Dvi," 2012, no. 1, pp. 1–14.
- [6] C. L. Tsai, C. J. Chen, and D. J. Zhuang, "Secure OTP and biometric verification scheme for mobile banking," *Proc. - 2012 3rd FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput. Music 2012*, pp. 138–141.
- [7] A. Amran, S. M. Nasution, and F. Azmi, "Implementasi Algoritma Kriptografi pada Sistem Biometric Payment," *Implementasi Algoritma Kriptografi pada Sist. Biometric Paym.*, 2013, vol. 3, no. 1, pp. 1–10.
- [8] S. Guan, R. E. De Grande, and A. Boukerche, "A novel energy efficient platform based model to enable mobile Cloud applications," 2016 *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Agustus, pp. 914–919.
- [9] M. Azure, *Face API Azure Documentation*. 2017 .
- [10] X. Cao, Y. Wei, F. Wen, and J. Sun, "Face alignment by explicit shape regression," 2014 *Int. J. Comput. Vis.*, vol. 107, no. 2, pp. 177–190.
- [11] W. Zhang, "Online Invoicing System Based on QR Code Recognition and Cloud Storage," 2018 *Proc. 2018 2nd IEEE Adv. Inf. Manag. Commun. Electron. Autom. Control Conf. IMCEC 2018*, no. Imceec, pp. 2576–2579.
- [12] P. Tresadern *et al.*, "Mobile biometrics: Combined face and voice verification for a mobile platform," *IEEE Pervasive Comput.*, 2013, vol. 12, no. 1, pp. 79–87.
- [13] X. Sun and N. Ansari, "Green Cloudlet Network: A Sustainable Platform for Mobile Cloud Computing," 2017, *IEEE Trans. Cloud Comput.*, vol. XX, no. XX, pp. 1–14.
- [14] M. Stojmenovic, "Mobile cloud computing for biometric applications," 2012, *Proc. 2012 15th Int. Conf. Network-Based Inf. Syst. NBIS 2012*, pp. 654–659.
- [15] R. Stefan and S. Daniel, "Cryptography for Security and Privacy in Cloud Computing," 2014, Artech House Computer Security Library.
- [16] F. Omri, S. Foufou, R. Hamila, and M. Jarraya, "Cloud-based mobile system for biometrics authentication," 2013 *13th Int. Conf. ITS Telecommun. ITST 2013*, pp. 325–330, 2013.