Jurnal Sistem Komputer dan Kecerdasan Buatan
Vol. II No. 1 Tahun 2018

Sistem Kehadiran Menggunakan *Quick Respone Code* Dengan *Enkripsi Algorithm Message Digest* 5 dan *Vigenere Cipher* Pada SpeedCom IT Consulting

Yudi Wiharto[1], Ari Irawan[2]

[1]Prodi Teknik Informatika Universitas Budi Luhur Jakarta
[2]Prodi Sistem Informasi Tanri Abeng University Jakarta
visited.mymail@gmail.com[1], ari_irawan@tau.ac.id[2]

Diterima: 31 Agustus 2018
Disetujui: 26 September 2018

***Abstract*—The attendance system is a resource that must be available and needed by both government institutions and private institutions to start the initial operational activities in it. The presence of the current attendance media is very important considering its function is able to support the activities and implementation of work activities in it so that the media must be in an agency / company. Especially for SpeedCom IT Consulting, data collection and attendance reporting systems used so far use data processing applications with web-based internet facilities. This is considered less effective by the company, because employees can enter attendance anywhere and anytime. From this problem raises the idea of adding a Quick Response Code (QR Code) encrypted with MD5 and Vigenere Cipher, which later can carry out management and attendance data collection. Supported by the availability of local internet networks within the company, this application will be used as a media for attendance and recapitulation of employee attendance every month. With the QR Code as a company attendance media, there are no more games or cheating by employees in the attendance process and it is hoped that this application will make it easier for administrators to manage employee attendance so that the results of data reporting can be more accurate.**

***Index Terms*— Attendance System, Encryption, Decryption, QR code**

I. PENDAHULUAN

Data kehadiran memiliki peranan penting paling awal dalam menjalani kegiatan sehari hari terutama di lingkungan kerja seperti sekolah, universitas, pabrik, perkantoran dan tempat lain yang membutuhkan data kehadiran. Di dalam lingkungan kerja khususnya, data kehadiran karyawan atau pegawai sangat dibutuhkan sebagai perhitungan untuk memberikan honor bulanan. Sudah ada beberapa sistem kehadiran yang pernah ada seperti dengan cara konvensional yaitu dengan cara menghitung ada berapa orang yang hadir, setelah itu sistem kehadiran berkembang memakai teknologi internet, sebenarnya tidak jauh berbeda dengan konvensional yang berbeda hanya pada rekapitulasinya saja karena sistem sudah melakukan rekapitulasi kehadiran secara otomatis, setelah itu sistem kehadiran berkembang menjadi kehadiran menggunakan *finger print*, dimana *finger print* tidak jauh berbeda dengan sistem kehadiran yang pernah ada sebelumnya, *finger print* (Sidik jari) ibarat *barcode* diri manusia yang menandakan tidak ada pribadi yang sama dan mengharuskan kita melakukan kehadiran secara personal, maka dari itu semakin kecil kemungkinan melakukan kecurangan saat proses kehadiran. Penelitian sidik jari sudah dilakukan sejak masa lampau oleh Gonzales[7]. Penelitian ini berkembang menjadi sebuah disiplin ilmu yang disebut dengan *dermatoglysphics*, yakni ilmu yang mempelajari pola guratan kulit (sidik jari) pada telapak, tangan dan kaki. *Dermatoglysphics* berasal dari kata "derm" berarti kulit, dan "glyph" berarti ukuran[8]. Setelah itu sistem kehadiran berkembang dengan pesat dengan menggunakan *QR code*. *QR code* dulu dipakai hanya untuk pertemanan di sosial media, *QR code* sekarang sudah bisa diisi dengan data atau semacamnya kepada penerima sehingga data dapat dikirim melalui berbagai perangkat, *QR code* juga dapat dimanfaatkan sebagai sistem kehadiran, sistem kehadiran *QR code* sama dengan sistem kehadiran yang ada sebelumnya, perbedaannya adalah cara pemakaiannya hanya bisa melalui *handphone* pribadi yang bersifat personal, jadi kemungkinan untuk melakukan kecurangan saat proses kehadiran pun semakin kecil, maka dari itu

dibuatlah *QR code* untuk sistem kehadiran. Untuk lebih menjaga kerahasiaan data pribadi yang terdapat dalam *handphone* pengguna agar tidak disalah gunakan oleh orang yang tidak bertanggung jawab maka disematkan metode enkripsi MD5.

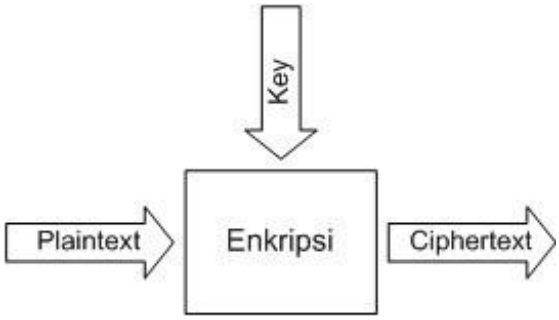
QRCode (Quick Respon Code) adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh *Denso Wave*, sebuah divisi *Denso Corporation* yang merupakan sebuah perusahaan Jepang dan dipublikasikan pada tahun 1994 dengan fungsionalitas utama yaitu dapat dengan mudah dibaca oleh pemindai QR merupakan singkatan dari *quick response* atau respons cepat, yang sesuai dengan tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula. Berbeda dengan kode batang, yang hanya menyimpan informasi secara horizontal, *QRCode* mampu menyimpan informasi secara horizontal dan vertikal, oleh karena itu secara otomatis *QRCode* dapat menampung informasi yang lebih banyak daripada *barcode*.(soon,2008)

Pada lingkungan kerja khususnya, kehadiran sangat dibutuhkan sebagai perhitungan honor bulanan karyawan. SpeedCom adalah perusahaan yang bergerak dibidang *IT Consulting* dengan sistem kehadiran menggunakan akses internet. Tetapi karyawan atau pegawai banyak yang tidak bertanggung jawab karena memanfaatkan kelemahan pada sistem kehadiran yang ada sekarang ini yang dapat diakses dimana dan kapan saja untuk menaikan honor yang dihitung dari lamanya waktu bekerja. Masalah yang ada pada SpeedCom yaitu karyawan yang bisa dengan mudah melakukan kehadiran kapan saja dan dimana saja, dengan begitu keamanan data karyawan pada sistem kehadiran juga belum bisa dianggap aman. Lalu bagaimana mengatasi karyawan yang melakukan kehadiran kapan saja dan dimana saja serta keamanan data karyawan pada sistem kehadiran juga belum bisa dianggap aman tersebut. Berdasarkan latar belakang masalah tersebut maka *QR code* adalah solusi baru yang akan digunakan sebagai sistem kehadiran yang baru. Dimana pada sistem kehadiran yang baru nantinya hanya bisa dipakai 1 orang untuk 1 *smartphone* dan sistem kehadiran ini bisa merekapitulasi kehadiran setiap bulan. Enkripsi yang akan digunakan pada sistem kehadiran ini hanya mengenkripsi IMEI *smartphone* dan data karyawan.

II. LANDASAN TEORI

A. Enkripsi

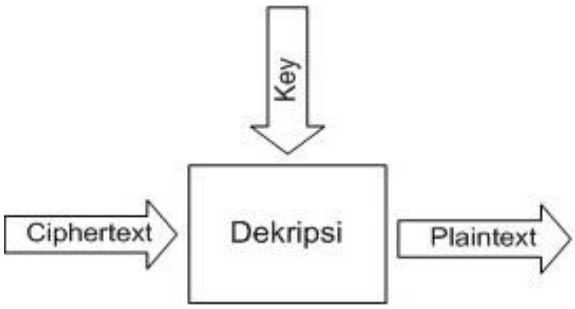
Enkripsi merupakan proses utama dalam suatu algoritma kriptografi adalah enkripsi dan dekripsi. Enkripsi merubah sebuah plaintext ke dalam bentuk ciphertext. Pada mode ECB (Elekctronic Codebook), sebuah blok pada plaintext dienkripsi ke dalam sebuah blok ciphertext dengan panjang blok yang sama. Blok cipher memiliki sifat bahwa setiap blok harus memiliki panjang yang sama (misalnya 128 bit). Namun apabila pesan yang dienkripsi memiliki panjang blok terakhir tidak tepat 128 bit, maka diperlukan mekanisme padding, yaitu penambahan bit-bit dummies untuk menggenapi menjadi panjang blok yang sesuai; biasanya padding dilakukan pada blok terakhir plaintext. Padding bada blok terakhir bisa dilakukan dengan berbagai macam cara, misalnya dengan penambahan bit-bit tertentu. Salah satu contoh penerapan padding dengan cara menambahkan jumlah total padding sebagai byte terakhir pada blok terakhir plaintext. Misalnya panjang blok adalah 128 bit (16 byte) dan pada blok terakhir terdiri dari 88 bit (11 byte) sehingga jumlah padding yang diperlukan adalah 5 byte, yaitu dengan menambahkan angka nol sebanyak 4 byte, kemudian menambahkan angka 5 sebanyak satu byte. Cara lain dapat juga menggunakan penambahan karakter *end-of-file* pada byte terakhir lalu diberi padding setelahnya [2].



Gambar 1. Proses Enkripsi

B. Dekripsi

Dekripsi merupakan proses kebalikan dari proses enkripsi, merubah ciphertext kembali ke dalam bentuk plaintext. Untuk menghilangkan padding yang diberikan pada saat proses enkripsi, dilakukan berdasarkan informasi jumlah padding yaitu angka pada byte terakhir setelahnya [3].



Gambar 2. Proses Dekripsi

C. *Keamanan Kriptografi*

Menurut Bruce Schneier, kriptografi adalah ilmu pengetahuan dan seni menjaga pesan agar tetap aman (*secure*). Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

a. *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

b. Data *integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

c. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

d. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Ada beberapa istilah-istilah yang penting dalam kriptografi, yaitu :

a. Pesan (*Plaintext* dan *Ciphertext*) : Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli disebut *plainteks* (*plaintext*) atau teks-jelas (*cleartext*). Sedangkan pesan yang sudah disandikan disebut cipherteks (*chipertext*).

b. Pengirim dan Penerima : Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitasyang menerima pesan

c. Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan.

d. Kriptanalisis dan Kriptologi : Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan *chiperteks* menjadi *plainteks* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

e. Enkripsi dan Dekripsi : Proses menyandikan *plainteks* menjadi *cipherteks* disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan cipherteks menjadi *plainteks* semula dinamakan dekripsi (*decryption*) atau *deciphering*.

f. *Cipher* dan Kunci : Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kunci (*key*) adalah parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*. Kunci biasanya berupa string atau deretan bilangan.

D. *Algorithm Message Digest 5 (MD5)*

Merupakan singkatan dari *Message Digest algortihm* 5, adalah fungsi hash (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografik yang digunakan secara luas dengan hash value 128-bit. MD5 dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk meguji integritas sebuah file. Enkripsi menggunakan MD5 masih mendominasi sebagian besar aplikasi PHP. Enkripsi MD5 dianggap strong karena enkripsi yang dihasilkannya bersifat '*one way hash'*. Berapa pun string yang di enkripsi hasilnya tetap sepanjang 32 karakter [4]. Message Digest 5 (MD5) juga merupakan salah satu dari

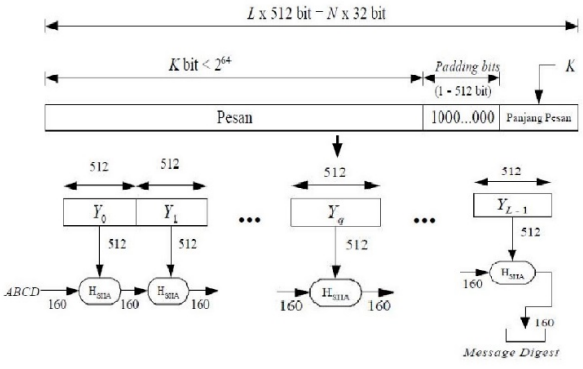
serangkaian *algoritma Message Digest* yang didesain oleh Professor Ronald Rivest dari MIT. Saat kerja analitik menunjukkan bahwa pendahulu MD5 -MD4- mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin). MD5 banyak digunakan pada bermacam macam aplikasi termasuk SSL/TLS, IPSec dan protokol-protokol kriptografi lainnya. MD5 juga biasa digunakan pada implementasi *Timestamping Mechanism, Commitment Schemes*, dan aplikasi pengecekan integritas pada *online software*. MD5 tidak memiliki sistem pengamanan seperti persamaan matematika, namun untuk setiap fungsi hash, domain D dan range R kita membutuhkan tiga hal berikut :

a. *Pre Image Resistance* : jika diberi suatu nilai y ε R, maka kita tidak akan dapat mencari suatu nilai x ε D dimana h(x)=y.

b. *Second Pre Image Resistance* : jika diberi suatu nilai x ε D, maka kita tidak akan dapat mencari nilai x' ε D dimana h(x)=h(x').

c. *Collision Resistance* : kita tidak akan dapat mencari nilai x,x' ε D dimana h(x)=h(x').

Fungsi hash yang banyak digunakan dalam kriptografi MD5 ini fungsi hash yang digunakan algoritma MD5. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit . Langkah-langkah dalam pembuatan *message digest* secara garis besar adalah sebagai berikut:



Gambar 3. Pembuatan *message digest* dengan algoritma MD5

Menilik dari gambar diatas, secara garis besar pembuatan message digest ditempuh melalui empat langkah, yaitu :

a. Penambahan bit-bit pengganjal (*padding bits*).

1 Pesan ditambah dengan sejumlah bit pengganjal sedemikian hingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512

2 Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah dari 1 sampai 512.

3 Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti beberapa sisanya bit 0.

b. Penambahan nilai panjang pesan semula.

1 Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.

2 Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah k bit, maka 64 bit yang ditambahkan menyatakan k modulo 264.

3 Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.

c. Inisialisasi penyangga (*buffer*) MD.

1 MD5 membutuhkan 4 buah penyangga (buffer) yang masingmasing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit.

2 Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut :

A= 01234567

B=89ABCDEF

C=FEDCBA98

D = 76543210

Pengolahan pesan dalam blok berukuran 512 bit. Proses berikutnya adalah pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (Y0 sampai YL1). Setelah itu setiap blok 512 bit diproses bersama dengan penyangga MD yang menghasilkan keluaran 128 bit, dan ini disebut HMD5.

E. *Vigenere Cipher*

Vigenere Chiper termasuk dalam cipher abjad majemuk (*polyalphabetic substitution Chiper*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise

de Vigenere pada abad 16 (tahun 1586). Vigenere Chiper adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Vigenere Chiper menggunakan tabel seperti pada tabel 1, Vigenere Cipher dengan angka. dalam melakukan enkripsi.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4. Tabel Vigenere Cipher dengan Angka

Jika ditukar dengan angka, maka kunci dengan huruf "HA" K = (7, 0, 17, 8)

Dan plaintextnya " SAYA HARIYANTO " akan menjadi P = (18, 0, 24, 0, 7, 0, 17, 8, 24, 0, 13, 19, 14).

S	A	Y	A	H	A	R	I	Y	A	N	T	O
18	0	24	0	7	0	17	8	24	0	13	19	14
7	0	17	8	7	0	17	8	7	0	17	8	7
25	0	16	8	14	0	9	16	6	0	5	2	21

Gambar 5. Tabel Vigenere Cipher Dengan Angka

Chipertext yang dihasilkan:

Chipertext = (25, 0, 16, 8, 14, 0, 9, 16, 6, 0, 5, 2, 2)

Chipertext yang dihasilkan dengan huruf menjadi "

Untuk melakukan deskripsi, bisa juga digunakan modulo 26)

Dari contoh tabel, maka dapat disimpulkan bahwa rumus dari enkripsi dan dekripsi data vigenere chiper adalah:

Enkripsi : Ci = (Pi + Ki) mod 26

Dekripsi : Pi = (Ci – Ki) mod 26;

untuk Ci > = Ki

Pi = (Ci + 67 – Ki) mod 26;

untuk Ci < = Ki

F. *QR Code*

QR code merupakan singkatan dari *Quick Respone code*, Permata kali digunakan di industri otomotif untuk melakukan *tracking* terhadap komponen kendaraan. Saat ini, penggunaan barcode dua dimensi ini sudah sangat luas, namun umumnya di pakai untuk mengkodekan alamat website, nomor contact, alamat email, nomor telepon atau sekedar teks biasa. Alat yang digunakan untuk membaca QR Code disebut *QR Code Scanner*. Umumnya alat ini bukanlah alat terpisah, namun tersedia dalam bentuk aplikasi di *smartphone* seperti Android atau iPhone. Tujuan utama QR Code saat ini digunakan untuk memudahkan pengguna *Smartphone* mengakses informasi dengan dua langkah mudah:

1 scan QR code
2 lakukan Aksi.

Aksi disini bisa berupa membuka browser, menyimpan informasi kontak, atau mendial nomor yang ada di QR code tersebut. Untuk membaca pesan yang tersembunyi di QR Code kita bisa memanfaatkan aplikasi bernama QR Code scanner yang bertebaran di Android Market atau Appstore. Android sendiri mempunyai banyak sekali tool QR code scanner. Manfaat paling utama di *smartphone* adalah untuk memudahkan dalam mengakses informasi, sebagai contoh, kita mendapatkan kartu nama dari kenalan baru, didalam kartu nama tersebut terdapat berbagai macam informasi seperti no Telepon, alamat rumah,email dan informasi lainnya termasuk QR Code.

III. ANALISA MASALAH DAN RANCANGAN PROGRAM

Pada bagian ini penulis menganalisa data yang diperoleh selama penelitian di SpeedCom *IT Consulting*, dengan cara deskriptif yang berarti pengolahan dan pengembangan data yang diperoleh dari hasil studi pustaka, observasi serta wawancara sehingga masalah-masalah yang ada mendapatkan solusinya. Pada aplikasi program yang dibuat menggunakan *platform* Android dengan memanfaatkan Android SDK dari Android Studio berbasis *IDE open source*.

A. Analisis Masalah dan Solusi

a. Analisa Masalah

Analisa permasalahan pada *SpeedCom IT Consulting* adalah karyawan bisa dengan mudah melakukan kehadiran kapan saja dan bisa dilakukan dimana saja tanpa harus datang ke kantor. Sehingga jam kerja karyawan bisa ditambahkan yang membuat honor karyawan

lebih tinggi dari yang seharusnya didapatkan. Selain itu masalah keamanan data karyawan yang kurang aman pada sistem sebelumnya.

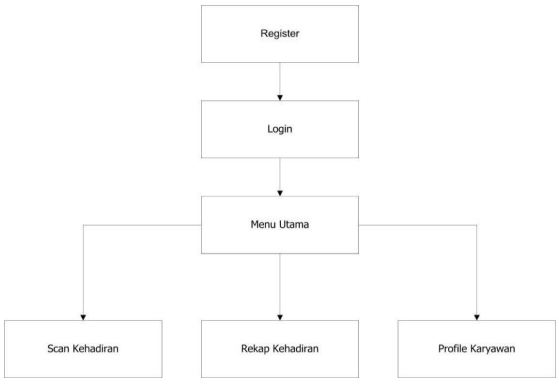
b. Solusi

Dari permasalahan diatas maka dibutuhkan sebuah aplikasi sistem kehadiran dengan proses *QR code* yang terenkripsi. Salah satu algoritma enkripsi yang cukup dikenal adalah algoritma enkripsi MD5 dan algoritma *Vignere Cipher* untuk enkripsi dan dekripsi data karyawan. Proses sistem kehadiran pada umumnya sebagai berikut:

1) Karyawan mendaftarkan dirinya di sistem kehadiran.
2) Aplikasi akan mengambil data karyawan dan memprosesnya untuk melakukan enkripsi
3) Karyawan yang sudah terdaftar, dapat langsung melakukan *scan* kehadiran di *web* yang berisi *QRcode* untuk melakukan kehadiran.
4) Hasil enkripsi berupa susunan tulisan kombinasi antara huruf, angka dan simbol acak yang tersimpan di database
5) Hasil dekripsi akan ditampilkan pada menu data karyawan berupa profile karyawan

B. Rancangan Menu

Rancangan menu dibuat untuk menganalisa menu yang terdapat pada bagianbagiannya, sehingga ketika terdapat masalah pada menu tersebut dapat kita telusuri dalam perbaikan aplikasi. Rancangan struktur menu yang dibuat disajikan dalam bentuk gambar sebagai berikut:



Gambar 6. Rancangan Struktur Menu

Menggunakan tampilan halaman standar, karena membutuhkan sebuah aplikasi yang responsif dalam keadaan mendesak merahasiakan sebuah SMS. Dalam rancangan tersebut akan memiliki 6 (enam) jumlah menu, yaitu:

1) Menu Register : merupakan menu yang digunakan untuk mendaftar pengguna yang akan menggunakan aplikasi.
2) Menu Login : merupakan menu yang digunakan untuk mencegah pengguna yang tidak bertanggung jawab menggunakan aplikasi.
3) Menu Utama : merupakan menu yang digunakan sebagai tampilan utama yang berisi menu menu dalam aplikasi.
4) Menu Scan Kehadiran : merupakan menu yang digunakan untuk melakukan scan kehadiran.
5) Menu Rekap Kehadiran : merupakan menu yang berisi untuk merekap kehadiran user setiap bulan.
6) Menu Profile Karyawan : merupakan menu yang berisi profile dari user.

C. Algoritma Program

Algoritma digunakan untuk mempermudah dalam pembuatan dan perancangan suatu sistem. Algoritma yang telah dibuat adalah terjemahan dari flowchart , dimana algoritma ini akan menjabarkan cara kerja program. Berikut ini akan dijelaskan algoritma proses aplikasi yang dikelompokkan dalam beberapa proses dan fungsi masing-masing sebagai berikut :

a.Algoritma Form Menu Register

Algoritma Menu Register adalah proses pada aplikasi ini untuk pengguna yang akan mendaftar. Berikut adalah Algoritma pada Menu register:

1. Tampil Form Registrasi
2. Input Form Biodata
3. If Form Biodata = Valid Then
4. Enkripsi Biodata dengan Vigenere Cipher
5. Simpan Imei dan Biodata
6. Tampil Menu Utama
7. Else
8. Tampil Pesan “Biodata Salah”
9. End if

b. Algoritma Form Menu Login

Algoritma Menu Login adalah proses pada aplikasi ini untuk masuk kedalam Menu. Berikut adalah Algoritma pada Menu Login:

1. Start
2. Tampilkan form login
3. Input imei
4. Hash Imei dengan MD5
5. If Imei = Valid Then
6. Tampil Form Menu Utama
7. Else
8. Tampil Form Registrasi
9. End if

c. Algoritma Form Menu Utama

Algoritma Menu Utama adalah proses pada aplikasi ini untuk memilih proses Scan, Menu Rekap, dan Menu Profil. Berikut adalah Algoritma pada Menu Utama :

1. Tampil Menu Utama
2. Input Action
3. If Action “Scan" Then
4. Tampil Form Scan
5. Else if Action “Menu Rekap” Then
6. Tampil Form Menu Rekap
7. Else if Action “Menu Profil” Then
8. Tampil Form Menu Profil
9. End if

d. Algoritma Form Menu Scan Kehadiran

Algoritma Menu Scan Kehadiran adalah proses pada aplikasi ini untuk memindai QR Code pada website dan menyimpan data berupa waktu masuk, waktu keluar, tanggal dan selisih waktu. Berikut adalah

Algoritma pada Menu Scan Kehadiran:

1. Tampil Form Scan
2. Input QR Code
3. If QR Code = Valid Then
4. Input Waktu dan Tanggal
5. If Label Waktu = Kosong Then
6. Input Waktu ke Label Waktu
7. Input Tanggal ke Label Tanggal
8. Kembali ke Menu Utama
9. Else
10. Input Waktu ke Label Keluar
11. Hitung Selisih Waktu Masuk dan
12. Keluar
13. Simpan Waktu Masuk, Waktu
14. Keluar, Selisih Waktu dan Tanggal
15. Kembali ke Menu Utama
16. End if
17. Else
18. Tampil Pesan “Scan Gagal”
19. Kembali ke Menu Utama
20. End if

e. Algoritma Form Menu Profil Karyawan

Algoritma Menu Profil Karyawan adalah proses pada aplikasi ini untuk menampilkan biodata karyawan berupa id, nama, email, nomor telepon, no ktp, tanggal lahir, dan alamat karyawan yang telah didekripsi dari database. Berikut adalah Algoritma pada Menu Profil Karyawan :

Tampilkan Form Menu Profil

1. Mengambil Data Biodata dari Database
2. Dekripsi Biodata dengan Vigenere Cipher
3. Tampilkan Biodata di Form Profil
4. Kembali ke Baris 1

f. Algoritma Proses MD5

Algoritma Proses MD5 adalah proses pada aplikasi ini untuk melakukan hashing data pada IMEI yang ada di handphone user. Berikut adalah Algoritma pada Menu Proses MD5 :

1. Start
2. Mengambil panjang pesan
3. Penambahan bit-bit pengganjal (Padding Bits)
4. Penambahan nilai panjang pesan semula
5. Inisialisasi Penyangga (Buffer) MD.
6. End

g. Algoritma Proses Vignere Cipher

Algoritma Proses *Vigenere Cipher* adalah proses pada aplikasi ini untuk melakukan enkripsi data karyawan . Berikut adalah Algoritma pada Proses *Vigenere Cipher* :

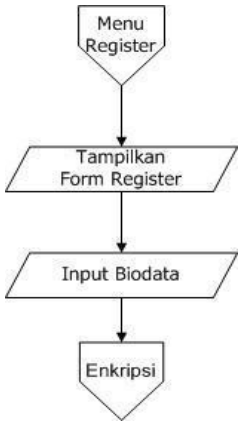
1. Start
2. Masukan Kunci
3. Jika Enkripsi maka hitung C=(P+K) mod 26
4. Menampilkan Ciphertext
5. Jika Dekripsi maka hitung P=(C-K) mod 26
6. Menampilkan Plaintext
7. End

D. Flowchart

Flowchart adalah diagram dengan simbol-simbol grafis yang menyatakan aliran algoritma atau proses yang menampilkan langkah-langkah yang disimbolkan dalam bentuk kotak, beserta urutannya dengan menghubungkan masing-masing langkah tersebut menggunakan tanda panah. Berikut ini adalah flowchart menu-menu yang terdapat pada aplikasi :

a. Flowchart Menu Register

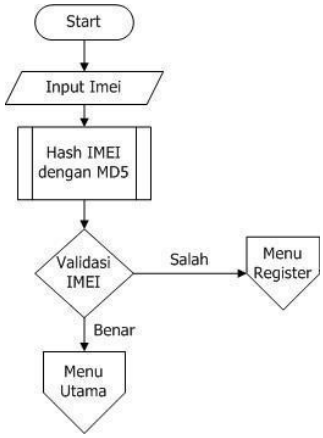
FlowChart Menu Register adalah proses aplikasi sistem ini untuk pengguna yang akan mendaftar. Flowchart dapat dilihat pada gambar berikut :



Gambar 7. Flowchart Menu Register

b.Flowchart Menu Login

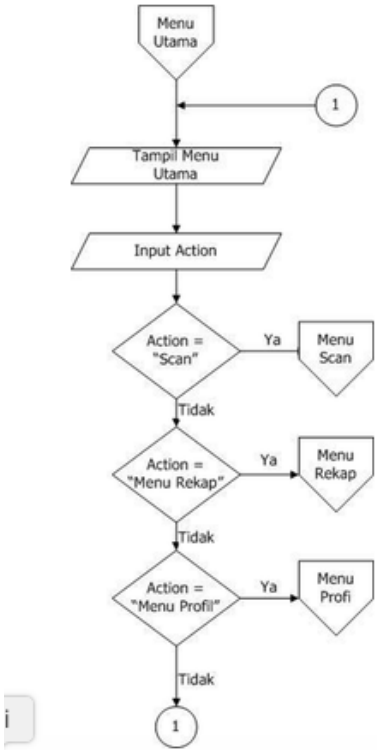
FlowChart Menu Login adalah proses aplikasi sistem keamanan data simetris dimana pengguna (anggota) dapat masuk ke halaman menu utama. Flowchart dapat dilihat pada gambar berikut :



Gambar 8. Flowchart Menu Login

c.Flowchart Menu Utama

FlowChart Menu Utama adalah proses aplikasi dalam memilih menu yang akan dibuka untuk melakukan sistem kehadiran. Flowchart dapat dilihat pada gambar berikut :

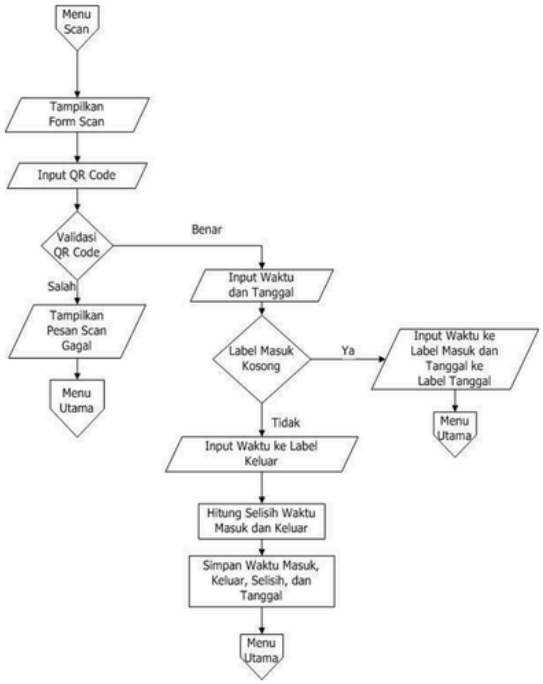


Gambar 9. Flowchart Menu Utama

d.Flowchart Menu Scan Kehadiran

Flowchart Menu Scan Kehadiran merupakan proses mengenkripsi pesan dengan menggunakan

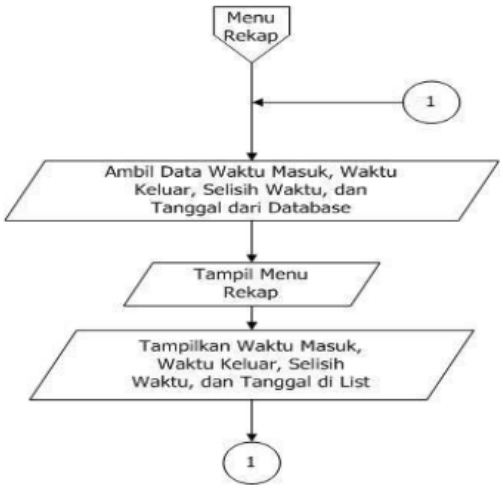
fitur SMS. Flowchart dapat dilihat pada gambar berikut:



Gambar 10. Flowchart Menu Scan Kehadiran

e.Flowchart Menu Rekap Kehadiran

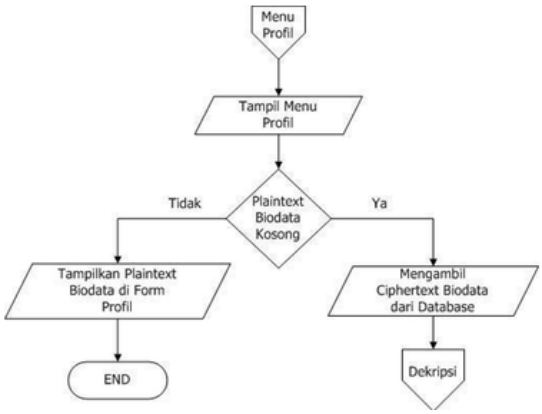
Flowchart Menu Rekap Kehadiran merupakan proses membaca rekap kehadiran. Flowchart dapat dilihat pada gambar berikut:



Gambar 11. Flowchart Menu Rekap Kehadiran

f.Flowchart Menu Profil Karyawan

Flowchart Menu Enkripsi merupakan prosen dari dekripsi Algoritma Vignere Cipher. Flowchart dapat dilihat pada gambar berikut :



Gambar 12. Flowchart Menu Profil Karyawan

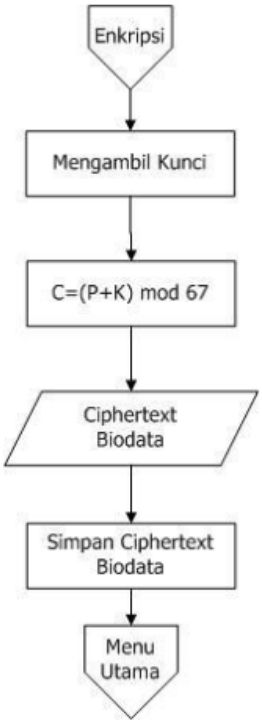
g.Flowchart Proses MD5

Flowchart Proses MD5 merupakan proses dari hashing data. Flowchart dapat dilihat pada gambar berikut:

Gambar 13. Flowchart Proses MD5

h.Flowchart Proses Enkripsi Vignere Cipher

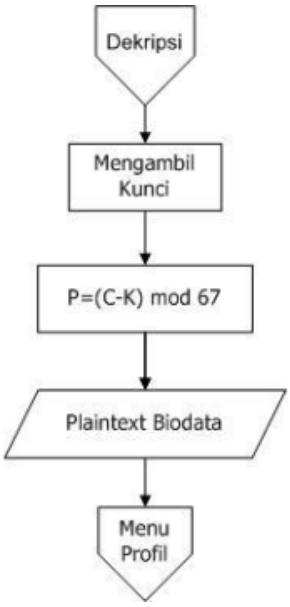
Flowchart Proses enkripsi *Vigenere Cipher* merupakan proses dari enkripsi data. Flowchart dapat dilihat pada gambar berikut :



Gambar 14. Flowchart Proses Enkripsi *Vigenere Cipher*

i. lowchart Proses Dekripsi Vignere Cipher

Flowchart Proses dekripsi *Vigenere Cipher* merupakan proses dari dekripsi data. Flowchart dapat dilihat pada gambar berikut:



Gambar 15. Flowchart Proses Dekripsi Vigenere Ciphe

IV. MPLEMENTASI DAN HASIL

A. *Lingkungan Percobaan*

Untuk mengimplementasikan aplikasi sistem kehadiran yang menjadi pembahasan utama pada penelitian ini dibutuhkan perangkat keras dan perangkat lunak untuk menjalankan aplikasi yang telah dibangun. Pada lingkungan percobaan akan dijelaskan mengenai spesifikasi dalam membuat aplikasi dan menjalankan aplikasi sesuai kebutuhan dengan spesifikasi minimum pada tahapan sebagai berikut:

a**.** Spesifikasi PC (Personal Computer) / Laptop

Dalam membuat aplikasi, penulis menggunakan perangkat lunak dan spesifikasinya yang digunakan sebagai berikut :

1) Perangkat lunak Android Studio 2.2.3
2) Java JDK dan paket OS Android 4.3
3) Processor i3 Quad-Core dengan minimum 1.80 Ghz (Giga Hertz) clock
4) RAM (*Random Access Memory*) minimum 8 GB (Giga Byte)

b. Spesifikasi Aplikasi *Smartphone*

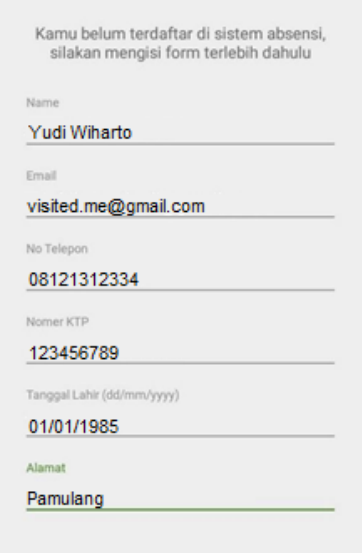
Untuk mendukung kelancaran aplikasi yang dibuat, maka sistem ini memerlukan *smartphone* dengan platform Android dalam penggunaannya. Adapun spesifikasi perangkat *smartphone* yang digunakan adalah sebagai berikut:

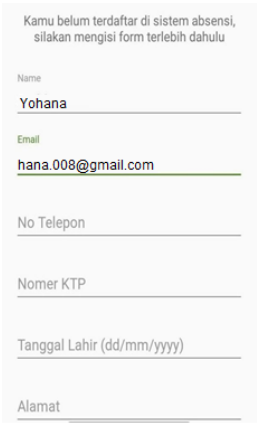
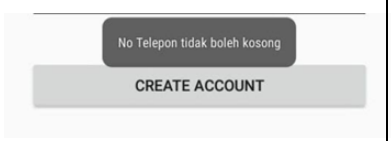
1) Sistem operasi Android minimum 4.3 JellyBean
2) Memori internal dibutuhkan 7 MB (Mega Byte)
3) RAM (*Random Access Memory*) minimum 512 MB

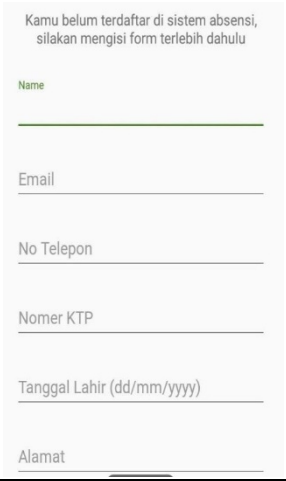
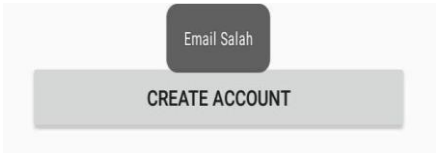
B. *Tabel Pengujian Register dan Scan Kehadiran*

a. Register dan Login

Tabel 1. Pengujian Verifikasi Register dan Login

Kasus dan Hasil Uji (Data Normal)		Tampil
Data masukan	Nama : Yudi Wiharto Email:visited.me@gmail.com No Telepon:08121312334 No KTP:123456789 Tgl Lahir : 01/01/1985 Alamat :Pamulang	
Yang diharapkan	Data yang dimasukkan benar sehingga dapat masuk kedalam menu utama.	

Kasus dan Hasil Uji (Beberapa dikosongkan)		Tampil
Data masukan	Nama : Yohana Email:hana.008@gmail.com No Telepon: No KTP: Tgl Lahir : Alamat :	
Yang diharapkan	Setelah klik tombol create account maka muncul pesan Register gagal.	
Pengamatan	Muncul pesan bahwa No Telepon tidak boleh kosong.	
simpulan	Tidak sesuai dengan pengamatan	

Kasus dan Hasil Uji (Semua kosong)		Tampil
Data masukan	Nama : Email: No Telepon: No KTP: Tgl Lahir : Alamat :	
Yang diharapkan	Setelah klik tombol create account maka muncul pesan Register gagal	
Pengamatan	Muncul pesan bahwa Email Salah	
Kesimpulan	Tidak sesuai dengan yang diharapkan	

b. Scan Kehadiran

Tabel 2. Pengujian Scan Kehadiran

Kasus dan Hasil Uji (Data Normal)		Tampil
Data masukan	*QR code* sesuai dengan database.	
Yang diharapkan	Setelah scan, maka muncul pesan berhasil.	
Pengamatan	Muncul pesan, berhasil	
Kesimpulan	Sesuai dengan yang diharapkan	

Kasus dan Hasil Uji (Data Salah)		Tampil
Data masukan	*QR code* tidak sesuai dengan database	
Yang diharapkan	Setelah scan, akan muncul pesan gagal.	
Pengamatan	Muncul pesan gagal.	
Kesimpulan	Sesuai dengan yang diharapkan	

Kasus dan Hasil Uji (Cancel Scan)		Tampil
Data masukan	*QR code* sesuai dengan database	
Yang diharapkan	Setelah scan, lalu klik back pada device muncul pesan “You cancelled the scanning”	
Pengamatan	Muncul pesan “You cancelled the scanning.	:
Kesimpulan	Sesuai dengan yang diharapkan	

C. *Tabel Pengujian Enkripsi dan Dekripsi*

Dalam pengujian kali ini, akan dibahas perbandingan antara proses enkripsi dan dekripsi data yang diuji. Pengujiannya yaitu dengan membandingkan data setelah proses enkripsi dengan data setelah proses dekripsi.

1) Tabel Enkripsi

Berikut tabel hasil percobaan data yang sudah di hash menggunakan MD5 :

Tabel 3. Tabel Hash MD5

Plantext	**Hash MD5**
862756037594862	6d741ad3f24b531bde3f9b9775a4e2ab

Berikut adalah tabel karakter yang digunakan dalam menghitung enkripsi Vigenere Cipher

Tabel 4. Tabel Karakter Vigenere Cipher

a	**b**	**c**	**d**	**e**
0	1	2	3	4
f	**g**	**h**	**i**	**j**
5	6	7	8	9
k	**l**	**m**	**n**	**o**
10	11	12	13	14
p	**q**	**r**	**s**	**t**
15	16	17	18	19
u	**v**	**w**	**x**	**y**
20	21	22	23	24
z				
25				

Berikut tabel hasil percobaan data yang sudah di enkripsi menggunakan Vigenere Cipher dengan rincian antara lain: Plantext (P), key (K), Ciphertext ((P+K) mod 26).

Tabel 5. Tabel Enkripsi Vigenere Cipher

Plantext (P)	**Key (K)**	**Ciphertext (P+K) mod 26**
Yudi Wiharto	SPEEDCOM	Qjhm Zkvmjis
visited.me@gmail.com	SPEEDCOM	nxwmwgr.yw@vqeln.qae
0812 1312334	SPEEDCOM	14616 19685010
123456789	SPEEDCOM	2222222202
1/1/1985	SPEEDCOM	18 15 7940
Pamulang	SPEEDCOM	Hpqyocbs

2) **Tabel Dekripsi**

Berikut tabel hasil percobaan data yang sudah di dekripsi Vigenere Cipher dengan rincian antara lain: Ciphertext (C), key (K), Plantext (C-K) mod 26.

Tabel 6. Tabel Dekripsi Vigenere Cipher

Ciphertext (C)	**Key (K)**	**Plantext (C-K) mod 26**
Qjhm Zkvmjis	SPEEDCOM	Yudi Wiharto
nxwmwgr.yw@vqeln.qae	SPEEDCOM	visited.me@gmail.com
14616 19685010	SPEEDCOM	0812 1312334
2222222202	SPEEDCOM	123456789
18 15 7940	SPEEDCOM	1/1/1985
Hpqyocbs	SPEEDCOM	Pamulang

3) Evaluasi Program

Dalam tahapan implementasi dan ujicoba program pada 21 karyawan SpeedCom IT Consulting dengan metode wawancara yang dibuat pada dokumen lampiran, dapat dievaluasi data sebagai berikut :

a. Hasil Evaluasi

1) Pada pengujian aplikasi dilakukan pengujian hashing pada nomor IMEI yang menggunakan MD5, proses tersebut menghasilkan 32 karakter.
2) Pada pengujian aplikasi dilakukan pengujian enkripsi *Vigenere Cipher* pada biodata pengguna dimana proses tersebut menghasilkan *ciphertext*.
3) Hasil pengujian dekripsi pada *ciphertext* sesuai dengan *plaintext*.

b. Kelebihan

1) Mudah dipahami dengan persentase 70% atau sekitar 7 dari 10 orang anggota.
2) Aplikasi ringan tidak memakai memori internal yang besar maupun memori proses yang banyak (batasan memori internal skala 0 MB – 90 MB dan memori proses skala 0 MB – 90 MB per jam).
3) Aplikasi dapat digunakan dari OS 4.3 JellyBean sampai versi OS 6.0 Marshmellow dan akan terus mengikuti perkembangan OS Android.

c. Kekurangan

1) Tampilan kurang menarik menurut 3 orang.
2) Menginput nomor telepon secara manual.
3)

V. SIMPULAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan serta uji coba aplikasi kehadiran karyawan SpeedCom IT Consulting dapat disimpulkan sebagai berikut :

1) Aplikasi sistem kehadiran dapat diamankan dengan kriptografi algoritma MD5
2) Aplikasi ini tidak dapat dibuka oleh pihak luar selain karyawan SpeedCom IT Consulting yang tidak memiliki akun pada aplikasi
3) Sistem kehadiran yang dienkripsi pada aplikasi ini tidak dapat dibuka pada aplikasi lain.
4) Aplikasi kehadiran dengan sistem keamanan kriptografi algoritma MD5 sudah diuji coba dan program dinyatakan telah sesuai.

B. Saran

Pengembangan yang perlu dilakukan untuk penelitian berikutnya adalah sebagai berikut :

1) Aplikasi ini dapat menghitung honor/gaji karyawan SpeedCom sesuai dengan rekap kehadiran.
2) Aplikasi ini dapat digunakan di flatform lain.

DAFTAR PUSTAKA

[1] Apridiansyah, Y., & Rifqo, M. H. (2015). APLIKASI KEAMANAN LEMBAR HASIL STUDI MENGGUNAKAN ALGORITMA MESSAGE DIGEST, (September), 107–114.

[2] Arjana, P. H., Rahayu, T. P., Yakub, & Hariyanto. (2012). Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Sentika, 2012(Sentika), 164–169.

[3] Komarudin, & Riswaya, A. R. (2013). Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/Md5 Pada Koperasi Mitra Sejahtera Bandung.

[4] Jurnal Computech & Bisnis, 7(1), 30–41. Retrieved from http://jurnal.stmikmi.ac.id/index.php/jcb/article/view/99

[5] Nuddin, M. T., & Fithri, D. L. (2015). Sistem Absensi Asisten Dosen Menggunakan *QR code* Scanner Berbasis Android Pada Program Studi Sistem Informasi Universitas Muria Kudus. Prosiding SNATIF, 0(0), 303–310.

[6] Rusdianto, & Qashlim, A. (2016). Implementasi Algoritma Md5 Untuk Keamanan Dokumen. Jurnal Ilmiah Ilmu Komputer, 2(2), 10–16

[7] Gonzales.2010. Digital Image processing.

[8] Putra,darma.2008. Sistem Biometrika.Yogyakarta : Andi.