Sistem Presensi Dosen Menggunakan IMEI dan GPS *Smartphone* dengan Data Terenkripsi

Adriana Fanggidae[1], Yulianto Triwahyuadi Polly[2]

***Abstract*— The improvement of education quality is determined not only by student's attendance but also lecturer's attendance in class. In this paper, control system of lecturer's attendance has been developed. This system requires two types of users, which are administrator and lecturer. The administrator is responsible for data analysis and report. The lecturer confirms his/her attendance using smartphone by utilising IMEI (International Mobile Equipment Identity) and GPS (Global Positioning System). The security of the data flow in this attendance system is built using the stream cipher algorithm with three key randomization methods: odd parity Hamming code, tent map and session keys. Research finds that this contol system of lecturer's attendance is secure because of the following reasons. First, it has been built using three-tier architecture. Second, there is a security check from software system. And lastly data flow is encrypted with low correlation between plaintext and ciphertext. Furthermore, the sytem is reliable because when internet and/or GPS is lost, data between client and server is kept and is delivered once there is internet and/or GPS connection. Report of lecturer's attendance from this system is reliable and hence it is recommended to be used for lecturers' attendance report.**

***Intisari*— Perbaikan mutu pendidikan tidak hanya dipandang dari sisi kehadiran mahasiswa di kelas tetapi juga yang tidak kalah penting adalah kehadiran tatap muka dengan dosen di kelas. Sistem presensi ini hanya diperuntukkan bagi dua pengguna, yaitu admin dan dosen, di mana admin melakukan pengolahan data dan laporan, sedangkan dosen melakukan presensi melalui perangkat *smartphone* dengan memanfaatkan IMEI (*International Mobile Equipment Identity), dan GPS (Global Positioning System*). Keamanan aliran data dalam sistem presensi ini menggunakan algoritme *cipher* aliran dengan metode pengacakan kunci, yaitu: Hamming *code* paritas ganjil, *tent map*, dan *session keys*. Hasil penelitian menunjukkan bahwa sistem sudah cukup aman karena dibangun menggunakan arsitektur *three-tier*, adanya *security check* dari perangkat lunak sistem, dan aliran data terenkripsi dengan nilai korelasi antara *plaintext* dan *ciphertext* yang sangat lemah. Sistem presensi ini juga handal dalam mempertahankan komunikasi data antara *client* dan *server* selama terjadi pemutusan koneksi internet dan/atau GPS. Laporan pertemuan dosen ini dapat dijadikan masukan bagi *decision maker* dalam menentukan keabsahan perkuliahan.**

***Kata Kunci*— sistem presensi, *smartphone*, GPS, Hamming *code* paritas ganjil, *tent map*, *session keys*.**

I. PENDAHULUAN

Lembaga pendidikan tinggi di Indonesia umumnya memiliki izin untuk menyelenggarakan perkuliahan dalam bentuk tatap muka, di mana dosen dan mahasiswa langsung bertatap muka. Kehadiran dosen di dalam perkuliahan sangat penting, di mana pada saat inilah terjadi proses belajar mengajar atau transfer ilmu pengetahuan dari dosen ke mahasiswa. Banyak lembaga pendidikan tinggi mulai memperhatikan kehadiran dosen di dalam perkuliahan, salah satunya dengan mewajibkan dosen mengisi lembar *monitoring* perkuliahan yang telah dipersiapkan oleh bagian kepegawaian. Pengisian lembar *monitoring* tentu saja tidak luput dari kecurangan-kecurangan yang dapat saja dilakukan oleh dosen, dan kecurangan-kecurangan ini seringkali mendapat respons yang lambat dari pimpinan lembaga pendidikan tinggi, sehingga adanya pencitraan yang kurang baik bagi dosen di mata mahasiswa.

Penentuan posisi dalam ruangan menjadi penting bila ditinjau dari aspek kebutuhan pengguna untuk mengetahui posisinya dalam sebuah gedung [1], misalnya seorang dosen yang perlu diketahui posisinya dalam sebuah gedung kuliah saat sedang melakukan perkuliahan. Salah satu alternatif penentuan posisi dalam ruangan dapat dilakukan dengan memanfaatkan fasilitas GPS (*Global Positioning System*) yang ada pada perangkat *mobile*. GPS merupakan sebuah sistem penentu posisi dan navigasi secara global menggunakan satelit [2]. Hampir setiap orang memiliki perangkat *mobile* dalam mendukung komunikasi mereka sehari-hari. IMEI (*International Mobile Equipment Identity)* merupakan suatu nomor unik yang dimiliki oleh setiap perangkat *mobile* yang dapat dijadikan sebagai identitasnya. Pada makalah ini digunakan IMEI sebagai identitas dosen, dan teknologi GPS sebagai penanda kehadirannya di dalam perkuliahan. Keamanan komunikasi perangkat *mobile* perlu dijaga dari pihak-pihak yang tidak bertanggung jawab sehingga dalam makalah ini digunakan arsitektur *three-tier* dan algoritme *cipher* aliran. *Cipher* aliran merupakan salah satu algoritme kunci simetri modern yang sangat sederhana, yang mana tingkat keamanannya sangat tergantung pada pembangkitan aliran kunci. Pembangkitan kunci menggunakan fungsi *tent map* memiliki keunggulan yaitu mampu melakukan pemetaan grafik yang menunjukkan dinamika sistem yang kacau dan berhubungan dengan persamaan *nonlinear*.

II. METODOLOGI

A. Algoritma Cipher Aliran dengan Pengacakan Kunci

Algoritma *cipher* aliran beroperasi pada *plaintext* atau *ciphertext* dalam bentuk bit tunggal yang dienkripsi atau didekripsi bit per bit [3]-[5].

$$c_i = (p_i \oplus k_i) \quad (1)$$

$$p_i = (c_i \oplus k_i) \quad (2)$$

[1,2]*Dosen, Jurusan Ilmu Komputer Fakultas Sains dan Teknik Universitas Nusa Cendana, Jln. Adisucipto Penfui Kupang 85001 INDONESIA (tlp: 0380-881597; e-mail: adrianailkom@gmail.com, yulianto.triwahyuadi@gmail.com)*

Untuk memperoleh panjang kunci yang sama dengan panjang *plaintext* atau *ciphertext* maka dilakukan *padding* kunci dan Hamming *code* paritas ganjil. Algoritme Hamming *code* paritas ganjil [6], [7] adalah sebagai berikut.

a. Menandai semua posisi bit di 2^i (i = 0, 1, 2, ...) sebagai paritas bit. (posisi: 1, 2, 4, 8, ...).
b. Bit-bit yang tidak termasuk dalam paritas bit akan digunakan dalam mengkodekan data. (posisi: 3, 5, 6, 7, ...).
c. Menghitung paritas dari setiap paritas bit dengan cara:
   - Posisi 1: *check* 1 bit, *skip* 1 bit, *check* 1 bit, *skip* 1 bit, dan seterusnya. (1, 3, 5, 7, 9, ...).
   - Posisi 2: *check* 2 bit, *skip* 2 bit, *check* 2 bit, *skip* 2 bit, dan seterusnya. (2, 3, 6, 7, 10, 11, ...).
   - Dan seterusnya.
d. Set paritas bit dengan 1 jika jumlah 1 pada posisi yang diperiksa adalah ganjil, dan set paritas bit dengan 0 jika jumlah 1 pada posisi yang diperiksa adalah genap.

Hasil yang diperoleh dikenakan *tent map* yang merupakan salah satu fungsi dari *chaos* yang berperilaku acak. *Tent map* termasuk dalam pemetaan satu dimensi, artinya sistem sederhana yang mampu melakukan gerak tidak beraturan [8]-[12].

$$x_{k+1} = f(x_k) \tag{3}$$

dengan

$$f(x) = \begin{cases} x_k/p & if\ 0 \le x_k \le p \\ (1 - x_k)/(1 - p) & if\ p < x_k \le 1 \end{cases} \tag{4}$$

Nilai awal x_k atau x_0 ditentukan dengan menggunakan teknik *session keys* [13]-[15]:

$$x_0 = (x_{01} + x_{02} + ... + x_{0t}) \bmod 1 \tag{5}$$

$$k_i = k_1, k_2, ..., k_n \tag{6}$$

dengan $x_0 \in [0,1]$, n = panjang kunci, t = banyaknya potongan kunci. Setiap potongan (B_1, B_2, ..., B_t) akan berisi $s = \frac{n}{t}$ (dengan syarat n mod t = 0), $i = 1 \ldots n$ dan k_i mewakili 8 bit dari setiap karakter kunci.

$$\begin{aligned} B_j = {} & k_{s(j-1)+1,1} k_{s(j-1)+1,2} \ldots k_{s(j-1)+1,8} \\ & k_{s(j-1)+2,1} k_{s(j-1)+2,2} \ldots k_{s(j-1)+2,8} \\ & \ldots k_{s(j-1)+q,1} k_{s(j-1)+q,2} \ldots k_{s(j-1)+q,8} \end{aligned} \tag{7}$$

Dengan $j = 1...t$, $q = 1 \ldots s$, $k_{1,1}$ ... $k_{1,8}$ sampai dengan $k_{n,1}$ ... $k_{n,8}$ merupakan nilai biner (0 atau 1) dari setiap karakter kunci, karena setiap karakter kunci diwakili oleh 8 bit biner maka $l = t * 8$, maka nilai $x_{01}, x_{02}, \ldots, x_{0t}$ dapat dihitung menggunakan representasi biner:

$$\begin{aligned} x_{0j} = {} & (k_{s(j-1)+1,1} * 2^0 + k_{s(j-1)+1,2} * 2^1 + \ldots \\ & + k_{s(j-1)+1,8} * 2^7 + k_{s(j-1)+2,1} * 2^8 + \\ & k_{s(j-1)+2,2} * 2^9 + \ldots + k_{s(j-1)+2,8} * 2^{15} + \ldots \\ & + k_{s(j-1)+q,1} * 2^{l-8} + k_{s(j-1)+q,2} * 2^{l-7} + \ldots \\ & + k_{s(j-1)+q,8} * 2^{l-1})/2^l \end{aligned} \tag{8}$$

Hasil dari *tent map* dibawa ke bentuk karakter ASCII.

$$\begin{aligned} BaK_j &= int(x_j) \\ K_j &= BaK_j \ mod\ 256 \end{aligned} \tag{9}$$

Selanjutnya dilakukan pergesaran bit untuk membuatnya lebih teracak.

$$\begin{aligned} T_j &= digit\ terakhir(BaK_j) \\ geser_j &= T_j \ mod\ 8 \end{aligned} \tag{10}$$

B. Koefisien Korelasi

Koefisien korelasi digunakan untuk mengetahui bagaimana keeratan hubungan antara suatu variabel dengan variabel lain [16]. Koefisien korelasi (r_{xy}) dari dua buah peubah acak diskrit yang masing-masing beranggotakan n elemen dihitung dengan rumus [17]-[20].

$$r_{xy} = cov(x,y)/\sqrt{D(x)D(y)} \tag{11}$$

Yang dalam hal ini:

$$cov\ (x,y) = \tfrac{1}{n}\textstyle\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)]$$

$$E(x) = \tfrac{1}{n}\textstyle\sum_{i=1}^{n} x_i$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2$$

$$E(y) = \tfrac{1}{n}\textstyle\sum_{i=1}^{n} y_i$$

$$D(y) = \tfrac{1}{n}\textstyle\sum_{i=1}^{n}[y_i - E(y)]^2$$

Suatu teks dikatakan memiliki hubungan *linear* yang kuat dengan teks lainnya yaitu dengan ditandai oleh koefisien korelasinya yang tinggi (mendekati +1 atau -1) [21]. Enkripsi bertujuan membuat korelasi antara *plaintext* dan *ciphertext* menjadi lemah atau dengan kata lain membuat koefisien korelasinya mendekati nol [22], [23].

III. HASIL DAN PEMBAHASAN

Sebelum sistem presensi dikembangkan perlu dilakukan uji keamanan dari algoritme kriptografi yang dipilih, yaitu dengan menganalisis hasil *padding* kunci tanpa dan dengan penggunaan Hamming *code* paritas ganjil, serta menganalisis korelasi yang terjadi antara *plaintext* dan *ciphertext*.

Analisis hasil *padding* kunci tanpa dan dengan Hamming *code* paritas ganjil, dapat dilihat pada Tabel I.

Kunci "adri" hasil *padding* memiliki empat pola yang sama, hal ini sangat rawan untuk diserang, di mana jika kriptanalis dapat memiliki satu pola maka ia dapat mengetahui kunci yang digunakan *user* dalam mengenkripsi data. Kunci "adri" hasil *padding* dengan Hamming *code* paritas ganjil memiliki hasil yaitu dari keempat pola yang ada masih terdapat dua pola yang masih berulang. Akan tetapi dua pola berulang ini tidaklah sama dengan nilai biner dari kunci "adri", sehingga pengacakan kunci dengan Hamming *code* paritas ganjil bisa dikatakan sudah baik.

Analisis korelasi antara *plaintext* dan *ciphertext* dilakukan terhadap lima file teks, hasil pengujian dapat dilihat pada Tabel II.

TABEL I
HASIL *PADDING* KUNCI

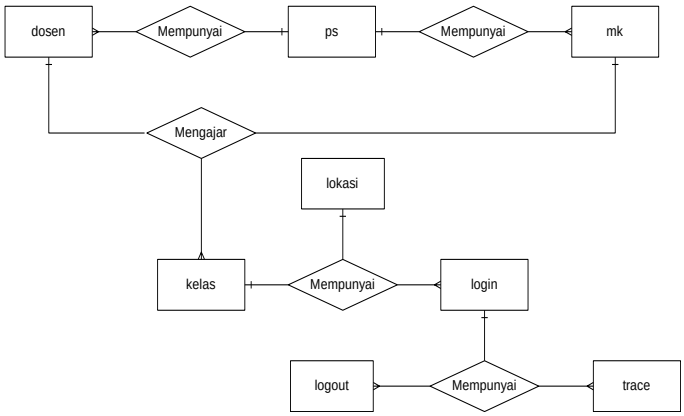
Kunci	a	d	r	i
ASCI	97	100	114	105
Biner	01100001	01100100	01110010	01101001
Kunci: 01100001011001000111001001101001 Total bit kunci = 32 Diinginkan kunci dengan panjang n = 128 bit dengan jumlah potongan kunci t = 4				
Hasil *padding* kunci tanpa Hamming *code* paritas ganjil: B_1 = 01100001011001000111001001101001 B_2 = 01100001011001000111001001101001 B_3 = 01100001011001000111001001101001 B_4 = 01100001011001000111001001101001 Hasil *padding* kunci dengan Hamming *code* paritas ganjil: B_1 = 00001100000101110010001110010011 B_2 = 10100101100000101100100011100100 0 B_3 = 11010010110000101100100011100100 B_4 = 11010010110000101100100011100100				

TABEL II
KORELASI ANTARA *PLAINTEXT* DAN *CIPHERTEXT*

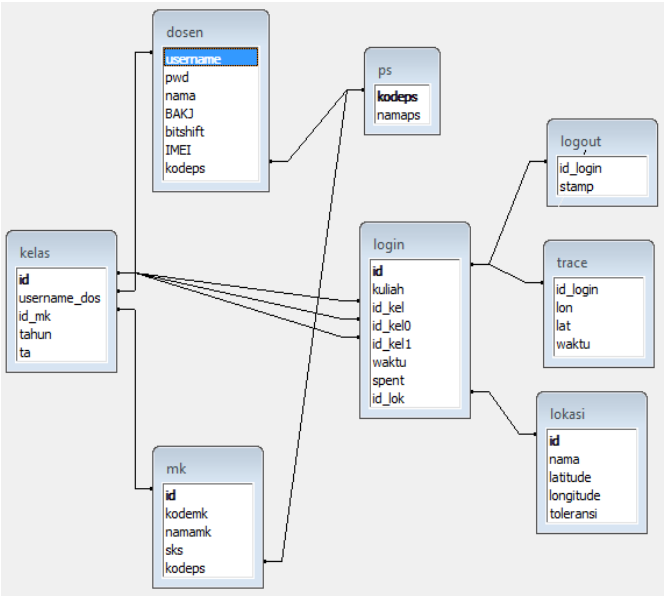
Nama File	**Korelasi (kunci: a)**	**Korelasi (kunci: adriana)**	**Korelasi (kunci: adrianafangidae)**
File_1	0,051623733	0,005586295	0,046072065
File_2	0,021686357	0,02992454	0,064486702
File_3	0,038395157	0,03590424	0,027819506
File_4	0,052340533	0,026072364	0,005001317
File_5	0,000574576	0,011775256	0,112768429
Rata-rata	0,032924071	0,021852539	0,051229604

Hasil enkripsi memperlihatkan bahwa nilai *absolute* dari korelasi mendekati nol. Ini menunjukkan bahwa korelasi antara *plaintext* dan *ciphertext* sangat lemah, sehingga dapat dikatakan metode yang dipilih sudah aman.

Sistem presensi yang dibangun diperuntukkan bagi perangkat *mobile* yaitu *smartphone* Android. Sistem ini menggunakan delapan tabel yang memiliki e*ntity relation diagram* (ERD) dan desain logis seperti yang terlihat pada Gbr. 1 dan Gbr. 2.



Gbr. 1 *Entity relation diagram.*

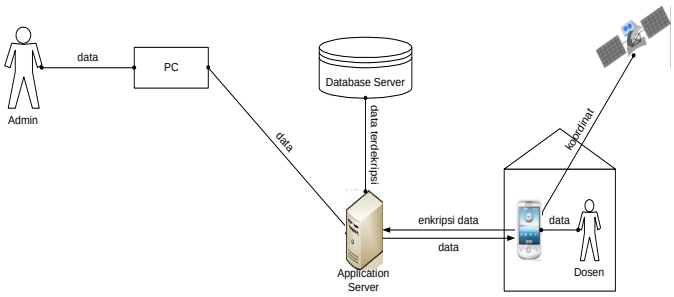


Gbr. 2 Desain logis.

Sistem ini memiliki aturan bisnis sebagai berikut:

- Dosen dari program studi "A" selain dapat mengajar di program studi "A" juga dapat mengajar di program studi lain.
- Dosen pengampu matakuliah "M" di beberapa kelas diperbolehkan melakukan perkuliahan gabungan maksimum hanya untuk tiga kelas.
- Panjang *password* yang digunakan maksimum 15 *byte*.
- Sistem presensi pada *smartphone* akan *logout* jika dosen melakukan *logout*.

Arsitektur dari sistem presensi ini dapat dilihat pada Gbr. 3.



Gbr. 3 Arsitektur umum sistem.

Pada Gbr. 3 dapat dijelaskan bahwa sistem yang dibangun terdiri atas dua sisi, yaitu:

- Sistem yang berjalan pada *desktop*.
  Sistem melakukan dua proses yaitu proses olah data dan laporan yang semuanya hanya dapat diakses oleh admin. Pada proses ini admin memasukan semua data yang dibutuhkan tabel ps, dosen, mk, lokasi, dan kelas.
- Sistem yang berjalan pada *smartphone*
  Sistem hanya melakukan proses presensi yang dapat diakses oleh dosen, saat sistem dijalankan maka dilakukan pemeriksaan sambungan internet dan GPS.

A. Algoritme Pemeriksaan Koneksi Internet

1. Membuat *broadcast* untuk memeriksa internet dan *register* ke *BroadcastReciever* untuk setiap *activity*.
2. Meminta servis internet dari *context* sekarang.
3. Jika servis internet tidak menyala dan koneksi tidak menyala maka:
   a. Membuat *dialog* untuk menyalakan internet.
   b. *Setting dialog* agar tidak dapat dibatalkan.
   c. *Setting* tombol *dialog* untuk mengarahkan *user* ke *setting* internet.
   d. Menampilkan *dialog.*

B. Algoritme Pemeriksaan Aplikasi GPS

1. Membuat *broadcast* untuk memeriksa GPS dan *register* ke *BroadcastReciever* untuk setiap *activity*.
2. Meminta servis lokasi dari *context* sekarang.
3. Jika servis GPS tidak menyala maka:
   a. Membuat *dialog* untuk menyalakan GPS.
   b. *Setting dialog* agar tidak dapat dibatalkan.
   c. *Setting* tombol *dialog* untuk mengarahkan *user* ke *setting* GPS.
   d. Menampilkan *dialog.*

Jika sambungan internet dan GPS telah aktif, proses *login* dapat dilanjutkan dengan memasukkan *username* dan *password*. Sistem akan mengambil nomor IMEI *smartphone* dan kode perangkat lunak yang digunakan, lalu semua data dienkripsi menggunakan *password* yang telah dimasukkan. Selanjutnya data tersebut didekripsikan kembali untuk diperiksa kebenarannya dengan data yang ada pada tabel dosen. Format *plaintext* saat *login* adalah

{username:”xxx“,password:”xxx”;imei:”xxx”;jws:”xxx”}

C. Algoritme Memeriksa Perangkat Lunak (Smartphone)

1. Menghubungkan aplikasi ke *google play service.*
2. Jika terhubung, maka:
   a. Meminta *SafetyNet* untuk memeriksa perangkat lunak dan mengembalikan *jws string.*
   b. Mengirim ke *server*, dan menunggu jawaban apakah perangkat lunak *valid.*
3. Jika tidak terhubung maka periksa kesalahan dan tampilkan kesalahan ke *user.*

D. Algoritme Memeriksa Perangkat Lunak (Server)

1. Menerima masukan berupa *string jws.*
2. Memeriksa integritas *string jws* apakah benar berasal dari *attest.google.*
3. Jika benar berasal dari *attest* maka:
   a. Memisahkan *jws* menjadi tiga bagian (keterangan *jws* dipisahkan dengan tanda titik).
   b. Mengambil bagian kedua dari *jws*, di-*decode*-kan dengan *base64 string.*
   c. Hasil *decode* berupa *String JSON*, di-*decode*-kan menjadi objek data.
   d. Memeriksa apakah objek data *package* sama dengan *package* aplikasi yang terdaftar.
   e. Memeriksa apakah objek data *sha256* sama dengan *sha256* yang digunakan untuk menandatangani aplikasi HP.
   f. Memeriksa apakah objek data *profile* CTS bernilai *true.*
   g. Memeriksa apakah waktu pemeriksaan masih dibawah tenggang waktu aman.
   h. Jika pemeriksaan benar maka:
      i. Mengembalikan hasil perangkat lunak *valid.*
      ii. Memberikan *token* akses.
   i. Jika tidak, maka hasil perangkat lunak tidak *valid* dikembalikan.
   j. Jika bukan berasal dari *attest* maka hasil perangkat lunak tidak *valid* dikembalikan.

E. Algoritme Security Check

1. Perangkat lunak yang *valid* saja yang bisa melakukan akses ke *server*
2. *Token* hanya berlaku untuk satu sesi *login* saja

Tampilan keberhasilan pemeriksaan keamanan sistem dapat dilihat pada Gbr. 4. Selanjutnya dosen dapat memilih matakuliah sesuai data yang ada pada tabel kelas dan lokasinya saat ini, seperti pada Gbr. 5.

Gbr. 4 Halaman *login* dan *security check*..

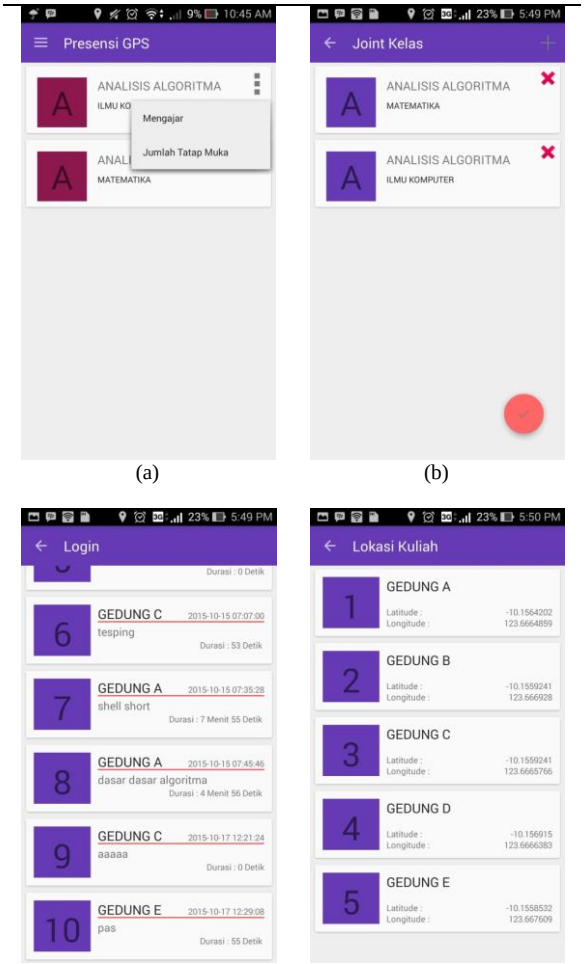
Data id_kelas, waktu, dan id_lokasi yang dimasukkan disimpan ke dalam tabel *login* sebagai penanda proses perkuliahan mulai dilakukan. Selama proses perkuliahan sistem akan secara rutin mengambil koordinat lokasi untuk disimpan ke dalam tabel *trace*. Jika proses perkuliahan selesai maka dosen dapat *logout* dari sistem. Proses enkripsi dan dekripsi data selalu dilakukan antara *client* dan *server* sepanjang komunikasi data berlangsung.

Selama perkuliahan, sistem presensi akan melakukan proses *ping* lokasi mengajar setiap 15 detik. Proses *ping* akan dihentikan secara otomatis jika jarak hasil *ping* ≤ jarak toleransi yang diberikan untuk setiap gedung atau jika sistem *logout*. Toleransi jarak yang diberikan untuk setiap gedung dapat dilihat pada Gbr. 6, dan halaman perhitungan durasi mengajar dapat dilihat pada Gbr. 7.

F. Algoritma Ping Lokasi Mengajar Selama Proses Perkuliahan (Smartphone)

1. Respon ← *ping*
2. Selama Respon = *ping*

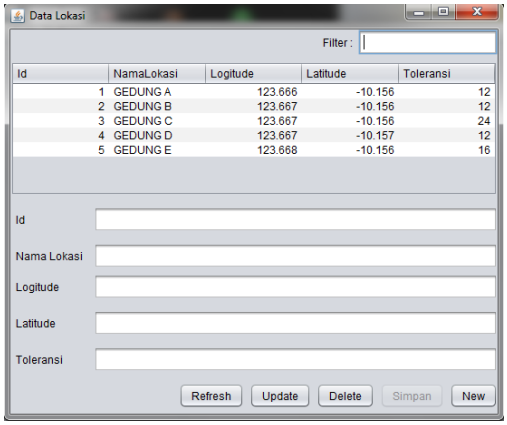
a. Minta lokasi dari gps
b. Jika lokasi tidak tersedia
   i. *Delay* 15 detik
   ii. Lanjutkan ke langkah 2
c. Jika lokasi tersedia
   i. *Delay* 15 detik
   ii. Kirimkan data lokasi ke *server*
   iii. Respon ← balasan dari *server* yaitu *ping* atau *stop*



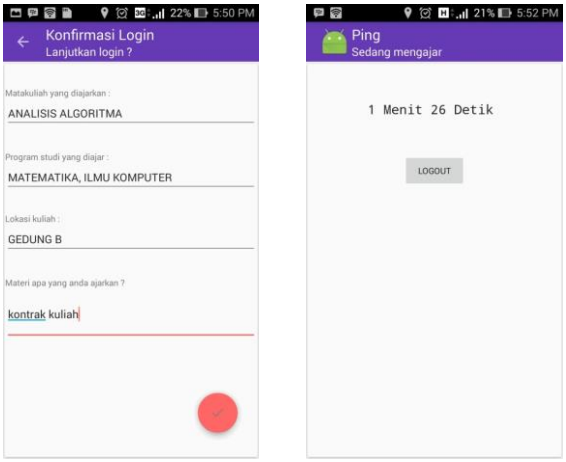
Gbr. 5 Halaman pemasukan data: (a) Halaman pemilihan matakuliah yang akan diajarkan (b) Halaman pemilihan penggabungan beberapa kelas dari matakuliah yang sama (c) Halaman jumlah tatap muka untuk suatu matakuliah (d) Halaman memilih lokasi kuliah yang digunakan.

G. *Algoritma Ping Lokasi Mengajar Selama Proses Perkuliahan (Server)*

1. Menerima data lokasi.
2. Jika jarak waktu lebih kecil 15 detik, respon *ping* dikirimkan.
3. Menyimpan data lokasi ke tabel *trace.*
4. Menghitung jarak lokasi dengan lokasi acuan.
5. Jika jarak lebih besar dari toleransi lokasi maka respon *ping* dikirimkan .
6. Jika jarak lebih kecil atau sama dengan toleransi lokasi maka respon *stop* dikirimkan.



Gbr. 6 Halaman lokasi gedung kuliah.

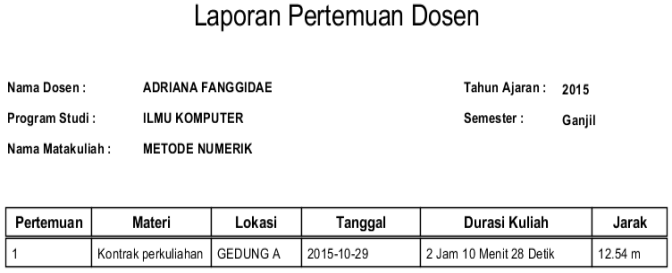


Gbr. 7 Halaman perhitungan durasi mengajar. (a) Halaman konfirmasi *login* (b) Halaman *ping* lokasi selama perkuliahan.

H. *Algoritma Ellipsiodal Distance*

1. Jari jari bumi r ← 6371
2. Selisih latitude ← Radian(*lat1-lat2*)
3. Selisih longitude ← Radian(*lon1-lon2*)
4. a ←sin(Selisih latitude / 2) * sin(Selisih latitude / 2)+cos(Radians(*lat1*)) *cos(Radians(*lat2*))* sin(Selisih longitude / 2) * sin(Selisih longitude / 2)
5. c = 2 * arctan(sqrt(a),sqrt(1 - a))
6. *jarak* = r * c

Algoritme e*llipsiodal distance* [24] digunakan dalam proses *ping* dan pelaporan pertemuan tatap muka untuk setiap dosen per matakuliah, seperti yang diperlihatkan pada Gbr. 8.


Laporan Pertemuan Dosen

Nama Dosen : ADRIANA FANGGIDAE
Tahun Ajaran : 2015
Program Studi : ILMU KOMPUTER
Semester : Ganjil
Nama Matakuliah : METODE NUMERIK

Pertemuan	Materi	Lokasi	Tanggal	Durasi Kuliah	Jarak
1	Kontrak perkuliahan	GEDUNG A	2015-10-29	2 Jam 10 Menit 28 Detik	12.54 m

Gbr. 8 Halaman laporan perkuliahan.

Pengujian dilakukan pada sistem presensi yang dibuat, yaitu pengujian fungsional dan non-fungsional. Pengujian ini bertujuan untuk melihat fungsional dan non-fungsional dari sistem yang dibuat. Hasil pengujian fungsional dan non-fungsional dari sistem presensi yang dibuat dapat dilihat pada Tabel III.

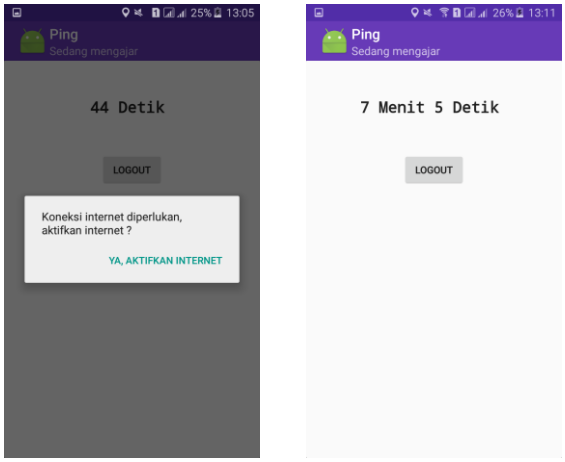
TABEL III
HASIL PENGUJIAN FUNGSIONAL DAN NON-FUNGSIONAL

Dekripsi	Kesimpulan
Melakukan *login* pada aplikasi *desktop* dengan masukan yang benar	Diterima
Melakukan *login* pada aplikasi *desktop* dengan masukan yang salah	Ditolak
Melakukan penambahan data program studi dengan masukan yang benar	Diterima
Melakukan penambahan data program studi dengan masukan yang salah	Ditolak
Melakukan pengubahan data program studi dengan masukan yang benar	Diterima
Melakukan pengubahan data program studi dengan masukan yang salah	Ditolak
Melakukan penghapusan data program studi	Diterima
Melakukan *refresh* data program studi	Diterima
Melakukan pencarian data program studi dengan masukan yang benar	Diterima
Melakukan pencarian data program studi dengan masukan yang salah	Ditolak
Melakukan penambahan data matakuliah dengan masukan yang benar	Diterima
Melakukan penambahan data matakuliah dengan masukan yang salah	Ditolak
Melakukan pengubahan data matakuliah dengan masukan yang benar	Diterima
Melakukan pengubahan data matakuliah dengan masukan yang salah	Ditolak
Melakukan penghapusan data matakuliah	Diterima
Melakukan *refresh* data matakuliah	Diterima
Melakukan pencarian data matakuliah dengan masukan yang benar	Diterima
Melakukan pencarian data matakuliah dengan masukan yang salah	Ditolak
Melakukan penambahan data dosen dengan masukan yang benar	Diterima
Melakukan penambahan data dosen dengan masukan yang salah	Ditolak
Melakukan pengubahan data dosen dengan masukan yang benar	Diterima
Melakukan pengubahan data dosen dengan masukan yang salah	Ditolak
Melakukan penghapusan data dosen	Diterima
Melakukan *refresh* data dosen	Diterima
Melakukan pencarian data dosen dengan masukan yang benar	Diterima
Melakukan pencarian data dosen dengan masukan yang salah	Ditolak
Melakukan penambahan data kelas dengan masukan yang benar	Diterima
Melakukan penambahan data kelas dengan masukan yang salah	Ditolak
Melakukan pengubahan data kelas dengan masukan yang benar	Diterima
Melakukan pengubahan data kelas dengan masukan yang salah	Ditolak
Melakukan penghapusan data kelas	Diterima
Melakukan *refresh* data kelas	Diterima
Melakukan penambahan data lokasi dengan masukan yang benar	Diterima
Melakukan penambahan data lokasi dengan masukan yang salah	Ditolak
Melakukan pengubahan data lokasi dengan masukan yang benar	Diterima
Melakukan pengubahan data lokasi dengan masukan yang salah	Ditolak
Melakukan penghapusan data lokasi	Diterima
Melakukan *refresh* data lokasi	Diterima
Melakukan pencarian data lokasi dengan masukan yang benar	Diterima
Melakukan pencarian data lokasi dengan masukan yang salah	Ditolak
Membuka aplikasi *smartphone* dengan keadaan sudah terkoneksi dengan internet	Diterima
Membuka aplikasi *smartphone* dengan keadaan belum terkoneksi dengan internet	Ditolak
Membuka aplikasi *smartphone* dengan keadaan GPS aktif	Diterima
Membuka aplikasi *smartphone* dengan keadaan GPS tidak aktif	Ditolak
Melakukan *login* pada aplikasi *smartphone* dengan masukan yang benar	Diterima
Melakukan *login* pada aplikasi *smartphone* dengan masukan yang salah	Ditolak
Melakukan presensi dengan menggunakan perangkat lunak yang sah	Diterima
Melakukan presensi dengan menggunakan perangkat lunak yang tidak sah	Ditolak
Melakukan presensi dengan IMEI yang telah tercatat pada tabel dosen	Diterima
Melakukan presensi dengan IMEI yang belum tercatat pada tabel dosen	Ditolak
Melakukan *logout* dari aplikasi *smartphone*	Diterima
Melihat data kehadiran dosen di kelas	Diterima

Pengujian kehandalan sistem meliputi beberapa hal sebagai berikut.

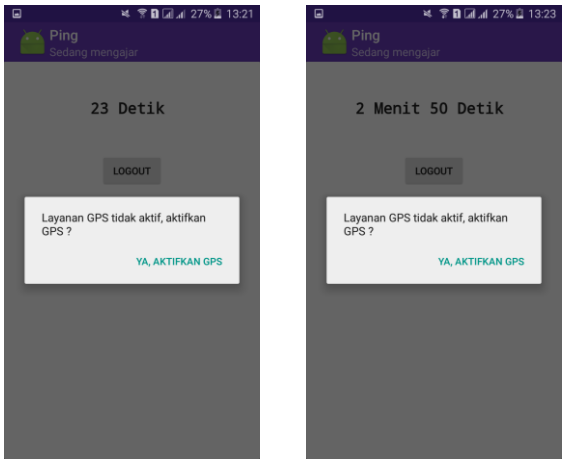
1) Kemampuan Sistem Mempertahankan Komunikasi Data: Pengujian dilakukan dengan memutuskan koneksi internet pada *smartphone* di tengah-tengah proses perkuliahan. Hasilnya diperoleh bahwa saat koneksi internet terhubung kembali, proses *ping* lokasi tetap dapat dilayani oleh *server* selama *client* belum melakukan *logout*. Hasil pengujian mempertahankan komunikasi data dapat dilihat pada Gbr. 9.

2) Kemampuan Sistem Mempertahankan Pembacaan Koordinat Lokasi: Pengujian dilakukan dengan memutuskan koneksi GPS pada *smartphone* di tengah-tengah proses perkuliahan, hasilnya diperoleh bahwa proses *ping* koordinat lokasi dari *client* ke *server* tetap dapat dilakukan selama perkuliahan dengan menggunakan pembacaan koordinat lokasi terakhir sebelum terjadi pemutusan. C*lient* dapat melakukan *logout* jika koneksi GPS terhubung kembali. Hasil pengujian mempertahankan pembacaan koordinat lokasi dapat dilihat pada Gbr. 10.

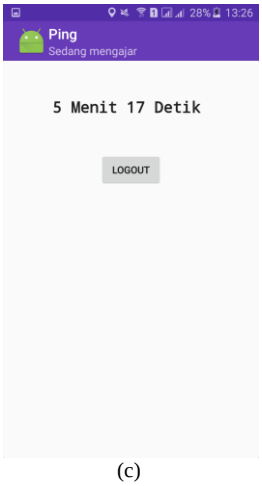


(a) (b)

Gbr. 9 Halaman pemutusan koneksi internet di tengah-tengah perkuliahan. (a) Halaman konfirmasi adanya pemutusan koneksi internet (b) Halaman koneksi internet terhubung kembali.



(a) (b)



(c)

Gbr. 10 Halaman pemutusan koneksi GPS di tengah-tengah perkuliahan. (a) Halaman konfirmasi pertama saat pemutusan koneksi GPS (b) Halaman konfirmasi masih terjadi pemutusan koneksi GPS (c) Halaman koneksi GPS terhubung kembali.

3) Kemampuan Sistem dalam Membaca GPS Smartphone. Pengujian dilakukan dengan melakukan presensi perkulihan di kelas yang ada pada lima gedung kuliah FST UNDANA. Hasil pengujian didapat seperti pada Tabel IV.

TABEL IV
HASIL PENGUJIAN PRESENSI PERKULIAHAN

Gedung	Jarak dari koordinat gedung
Gedung A	± 19 meter
Gedung B	± 40 meter
Gedung C	± 18 meter
Gedung D	± 39 meter
Gedung E	± 60 meter
Rata-rata	± 35,2 meter

Dari hasil pengujian pada Tabel IV diperoleh penyimpangan jarak dari koordinat gedung (sesuai data pada tabel lokasi) rata-rata sebesar ± 35,2 meter. Nilai ini dapat dijadikan jarak toleransi untuk setiap gedung agar selisih antara jarak toleransi dengan jarak rata-rata perkuliahan tidak terlalu jauh.

IV. KESIMPULAN

Dari hasil penelitian diketahui sistem presensi yang dibangun sudah cukup aman karena menggunakan aristektur *three-tier*, adanya *security check* dari perangkat lunak, dan aliran data terenkripsi dengan nilai rata-rata korelasi antara *plaintext* dan *ciphertext* yang mendekati nol. Sistem presensi juga mampu mempertahankan komunikasi antara *client* dan *server* selama terjadi pemutusan koneksi internet dan/atau GPS. Selain itu, laporan pertemuan dosen ini dapat dijadikan masukan bagi *decision maker* dalam menentukan keabsahan perkuliahan dengan memperhatikan selisih antara jarak toleransi dengan jarak yang terdapat pada laporan.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada KEMENRISTEKDIKTI atas pendanaannya sehingga penelitian ini dapat berjalan, dan tim JNTETI atas masukan dan sarannya.

REFERENSI

[1] Azkario Rizky Pratama and Widyawan, "Pedestrian Dead Reckoning pada Ponsel Cerdas sebagai Sistem Penentuan Posisi dalam Ruangan," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 2, no. 3, pp. 20-25, Agustus 2013.

[2] Teguh Firmansyah, Sabdo Purnomo, Feti Fatonah, and Tri Hendarto Fajar Nugroho, "Antena Mikrostrip Rectangular Patch 1575,42 MHz dengan Polarisasi Circular untuk Receiver GPS," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 4, no. 4, November 2015.

[3] Hongjun Wu, *Cryptanalysis And Design Of Stream Ciphers*. Belgium: B-3001 Heverlee, 2008.

[4] Christof Paar and Jan Pelzl, *Understanding Cryptography*. London New York: Springer-Verlag Berlin Heidelberg, 2010.

[5] Rick Wash. Lecture Notes on Stream Ciphers and RC4. [Online]. http://rickwash.com/papers/stream.pdf

[6] B. K. Gupta and R. L. Dua, "Communication by 31 Bit Hamming Code Transceiver with Even Parity and Odd Parity Check Method by Using VHDL," *IJECCT*, vol. 2, no. 4, 2012.

[7] Nutan Shep and P. H. Bhagat, "Implementation of Hamming code using VLSI," *International Journal of Engineering Trends and Technology*, vol. 4, no. 2, 2013.

[8] Rainer Klages. (2008, April) Introduction to Dynamical Systems. [Online]. http://www.maths.qmul.ac.uk/~klages/mas424/lnotes_ds2007f.pdf

[9] Adriana Vlad, Adiran Luca, Octavian Hodea, and Relu Tataru, "Generating Chaotic Secure Sequences Using Tent Map And A Running-Key Approach," in *Proceedings Of Romanian Academy, Series A*, vol. 14, 2013, pp. 295-302.

[10] Sarika Tyagi and Deepak Chaudhary, "Adapted Encryption Algorithm With Multiple Skew Tent Map," *IJCSM*, vol. 2, no. 4, pp. 422-428, April 2013.

[11] Wadia Faid Hassan Al-Shameri and Mohammed Abdulkawi Mahiub, "Some Dynamical Properties Of The Family Of Tent Maps," *Int. Jornal Of Math. Analysis*, vol. 7, no. 29, pp. 1433-1449, 2013.

[12] Justin Guo. (2014) Analysis Of Chaotic Systems. [Online]. http://Math.Uchicago.Edu/~May/Reu2014/Reupapers/Guo.Pdf

[13] N. K. Pareek, Vinod Patidar, and K. K. Sud. (2004) Cryptography Using Multiple One-Dimensional Chaotic Maps. [Online]. www.sciencedirect.com

[14] N. K. Pareek, Vinod Patidar, and K. K. Sud, "Image Encryption Using Chaotic Logistic Map," *Elsevier*, vol. 24, no. 9, pp. 926-934, 2006.

[15] P. Vidhya Saraswathi and M. Venkatesulu, "A Block Cipher For Multimedia Encryption Using Chaotic Maps For Key Generation," in *Proc. Of Int. Conf. on Advances In Information Technology And Mobile Communication*, 2013.

[16] Algifari , *Analisis Regresi Teori, Kasus dan Solusi*, 2nd ed. Yogyakarta: BPFE, 2013.

[17] Shujiang Xu, Yinglong Wang, Jizhi Wang, and Yucui Guo, "A Fast Image Encrytion Scheme Based On A Nonlinear Chaotic Map," in *2nd International Conference On Signal Processing Systems (ICSPS)*, 5-7 July 2010, pp. v2-326-v2-330.

[18] T. Hongmei, H. Liying, H. Yu, and W. Xia, "An Improved Compound Image Encryption Scheme," in *Proceeding of 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*, 2010.

[19] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based On Rubik's Cube Principle," *Journal Of Electircal And Computer Engineering*, vol. 2012, 2012.

[20] Mohid Kumar, Akshat Aggarwal, and Ankit Garg, "A Review On Various Digital Image Encryption Techniques And Security Criteria," *International Journal Of Computer Applications*, vol. 96, no. 13, pp. 19-26, 17 June 2013.

[21] Bruce Ratner, *Statistical and machine-learning data mining Techniques for better predictive modeling and analysis of big data*, 2nd ed.: CRC Press, Taylor & Francis Group, 2011.

[22] Obaida Mohammad Awad Al-Hazaimeh, "A New Approach For Complex Encrypting And Decrypting Data," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 5, no. 2, March 2013.

[23] Firas Shawkat Hamid, Thakwan Akram Jawad, and Ersun Iscioglu, "Study and Analysis New Algorithm for Effective Cryptographic in Telemedicine Purposes Using Hill Cipher after Modification," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 3, no. 3, February 2014.

[24] Andy McGovern. (2003) Geographic Distance and Azimuth Calculations. [Online]. http://www.codeguru.com/cpp/cpp/algorithms/article.php/c5115/Geographic-Distance-and-Azimuth-Calculations.htm