RANCANG BANGUN SIMULASI PEMANFAATAN METODE *INTERLOCK PROTOCOL* UNTUK MENGATASI *MAN-IN-THE-MIDDLE-ATTACK* BERBASIS DEKSTOP

Rudi Syah Putra
STMIK Kristen Neumann Medan JL.Jamin Ginting KM.10,5 Medan
Email : rudisyahputra01@gmail.com

Program Studi Teknik Informatika

ABSTRACT

In the process of data communication, even though the data has been encrypted, there is a possibility that the data can be known by others. One possibility is that the person intercepted the communication media used by the two people who were communicating. This is what is called man-in-the-middle-attack. This man-in-the-middle-attack problem can be prevented by using the interlock protocol. This interlock protocol was created by Ron Rivest and Adi Shamir. The core algorithm of this protocol is that it sends 2 encrypted messages. The first part can be the result of the one way hash function of the message and the second part is the encrypted message itself. This causes the intercepting person to be unable to decrypt the first message using his private key. He can only create a new message and send it to the person who will receive the message.

Keywords *: Communication, encryption, man-in-the-middle-attack*

1. PENDAHULUAN

Dalam proses komunikasi data, walaupun data telah dienkripsi, terdapat kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinan tersebut adalah orang tersebut menyadap media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi tersebut. Hal inilah yang disebut dengan *man-in-the-middle-attack*. Dalam keadaan ini, orang yang menyadap berada di antara kedua orang yang sedang berkomunikasi. Data-data yang dikirimkan oleh orang yang sedang berkomunikasi satu sama lain selalu melalui orang yang menyadap tersebut, sehingga orang yang menyadap tersebut dapat mengetahui semua informasi yang dikirimkan satu sama lain. Keadaan ini muncul karena kedua orang yang sedang berkomunikasi tersebut tidak dapat mem-verifikasi status dari orang yang berkomunikasi dengannya tersebut, dengan mengambil asumsi bahwa proses penyadapan tersebut tidak menyebabkan gangguan dalam jaringan.

Penulis merasa sangat tertarik untuk mempelajari problema *man-in-the-middle-attack* ini dan solusinya dengan menggunakan metode *interlock protocol*. Oleh karena itu, penulis mengambil tugas akhir (skripsi) dengan judul **"Simulasi Pemanfaatan Metode *Interlock Protocol* untuk mengatasi *Man-In-The-Middle-Attack*".**

Rumusan Masalah

Berdasarkan latar belakang pemilihan judul, maka yang menjadi permasalahan adalah bagaimana menjelaskan proses kerja *man-in-the-middle-attack* dalam menyadap dan mengubah pesan, menjelaskan proses kerja *interlock protocol* untuk mengatasi problema *Man-In-The-Middle-Attack*, menampilkan algoritma dari sistem kriptografi kunci

publik metode RSA dan merancang *interface* dari perangkat lunak simulasi.

1.3.Tujuan Penelitian

1. Untuk mengetahui bagaimana proses yang sedang berjalan
2. Untuk mengetahui kehadiran dosen dalam proses belajar mengajar
3. Merancang aplikasi sistem monitoring kehadiran dosen dalam proses belajar mengajar menggunakan aplikasi andriod.

1.4. Manfaat Penelitian

1. Membangun sistem monitoring kehadiran dosen dalam proses belajar mengajar
2. Agar meningkatkan disiplin dosen dalam proses belajar mengajar
3. Memberikan kemudahan bagi Dosen dan Pimpinan dalam melihat data kehadiran dosen dalam proses belajar.

2. LANDASAN TEORI

Sistem berasal dari bahasa Latin (*systēma*) dan bahasa Yunani (*sustēma*) adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi. Istilah ini sering dipergunakan untuk menggambarkan suatu set entitas yang berinteraksi, di mana suatu model matematika seringkali bisa dibuat.

Sistem adalah sekumpulan unsur / elemen yang saling berkaitan dan saling mempengaruhi dalam melakukan kegiatan bersama untuk mencapai suatu tujuan.

Secara umum Monitoring adalah kegiatan penilaian pola kerja yang dilakukan dengan cara mengkaji maupun mengamati sesuatu kegiatan yang dilaksanakan telah sesuai dengan rencana.

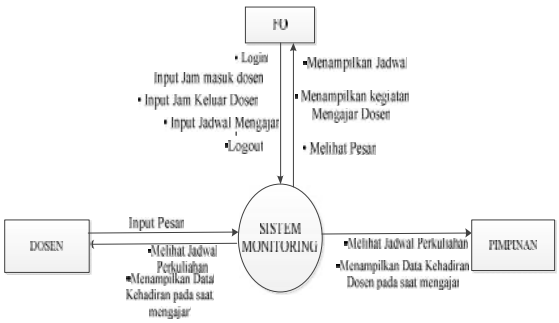
Android adalah operating system atau OS berbasis linux yang diperuntukan khusus untuk mobile device seperti smartphone atau PC table, persis seperti symbian yang dipergunakan oleh Nokia dan BlackBerry OS, jelasnya seperti microsoft windows yang sangat dikenal baik oleh para pengguna komputer dan laptop, jika kita analogikan, Andoid adalah windows nya sedangkan smartphone atau hand phone atau tablet adalah unit komputernya.

Android Studio adalah sebuah IDE untuk Android Development yang dikenalkan pihak google pada acara Google I/O di tahun 2013. Android Studio merupakan suatu pengembangan dari Eclipse IDE, dan dibuat berdasarkan IDE Java populer, yaitu IntelliJ IDEA. Android Studio merupakan IDE resmi untuk pengembangan aplikasi Android.

3. ANALISIS DAN PERANCANGAN

Sistem monitoring ini merupakan cara yang dilakukan oleh suatu instansi untuk mengetahui kegiatan apa yang sedang dilakukan. Dalam penelitian ini sistem monitoring (pemantauan) di tujukan kepada proses belajar mengajar di STMIK Neumann, dalam sistem ini aplikasi yang digunakan yaitu Aplikasi Android Studio. Dari aplikasi tersebut dapat memudahkan dosen, pimpinan dan fo dalam melihat atau memonitoring jadwal dan kegiatan mengajar dosen, apakah sudah sesuai dengan jadwal yang telah di tentukan atau tidak

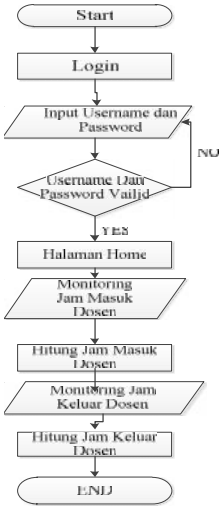
Diagram Konteks



Gambar 1. Diagram Konteks Perancangan Sistem Informasi Monitoring

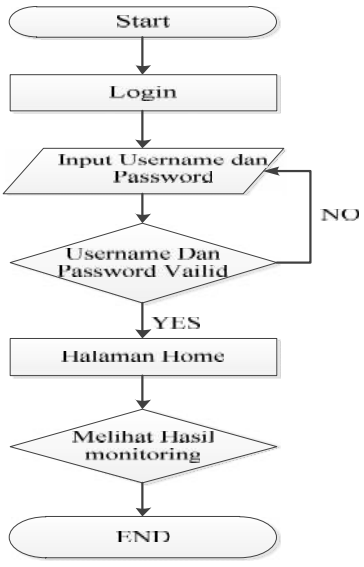
P-ISSN:2548 5997 E-ISSN : 2685-1768

Rancangan flowchart Admin



Gambar 2.*Flowchart* Admin

Rancangan Flowchart Dosen dan Pimpinan



Gambar 3. *Flowchart* Dosen dan Pimpinan

Tabel User

Tabel 1. tm_user

Field	Type	Size
Id_user	Varchar	10
Password	Varchar	100
Nama	Varchar	15
Hak_Akses	Varchar	4

Tabel Jadwal

Tabel 2. jadwal

Field Name	Type	Size
Id_jadwal	Int	6
Id_ta	Varchar	6
Id_prodi	Varchar	6
Id_kurikulum	Varchar	6
Id_mk	Varchar	10
Kelas	Varchar	15
Id_dosen	Varchar	15
Hari	Varchar	15
Jam_masuk	Time	
Jam_keluar	Time	

Tabel Prodi

Tabel 3 Prodi_data

Field Name	Type	Size
Id_Prodi	Varchar	2
Nama	Varchar	30
Jenjang	Varchar	15
Kaprodi	Varchar	50

Tabel Matakuliah

Tabel 4. kurikulum

Field Name	Type	Size
Id_mk	Int	6
Id_kurikulum	Int	6
Id_prodi	Varchar	6
Kode_mk	Varchar	10
Nama_mk	Varchar	60
Sks_mk	Int	3
Smt_mk	Varchar	4
Status	Varchar	30

Tabel T.A

Tabel 5. Tahun_akademik

Field Name	Type	Size
Id_ta	int	5
Ta	Varchar	15
semester	Varchar	15
id_user	Varchar	10
Status	char	10

Tabel Presensi

Tabel 6. tm_presensi_dosen

Field Name	Type	Size
id_log	Int	9
id_dosen	Varchar	12
id_jadwal	Int	7
Tanggal	date	
jam_masuk	Time	
jam_keluar	Time	
jam_masuk_r	Time	
jam_keluar_r	Time	
id_ruangan	Varchar	10
status_mengajar	varchar	10

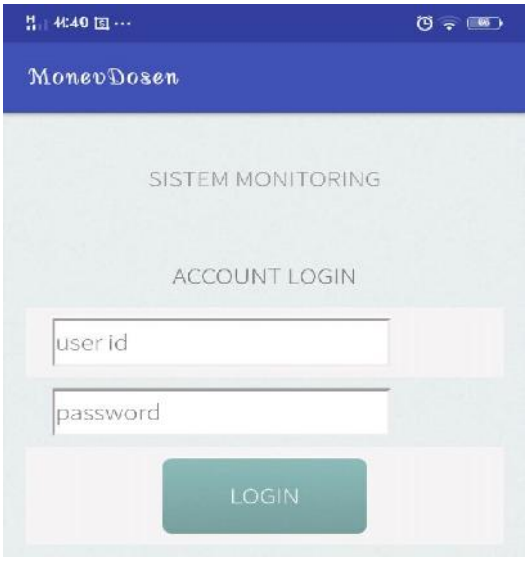
Tabel Dosen

Tabel 7. dosen_data

Field Name	Type	Size
Id_dosen	Int	10
Nidn	Varchar	40
Nama	Varchar	50
Devisi	Varchar	40
J_fungsional	Varchar	50
J_akademik	Varchar	50
Pendidikan	Varchar	10
J_kelamin	Varchar	15
Tempat	Varchar	50
Tgl_lahir	date	
Agama	Varchar	20
Alamat	Varchar	100

4. HASIL DAN PEMBAHASAN

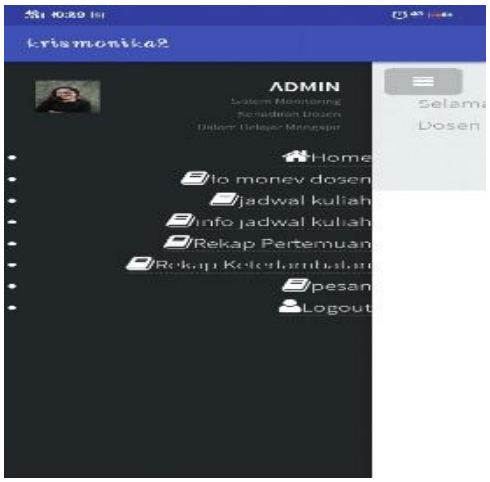
Form Menu Login



Gambar 3. Tampilan Halaman Login

Form Menu Fo

Berikut merupakan tampilan nama- nama menu yang ada dalam sistem tersebut :



Gambar 4. Tampilan Menu Fo

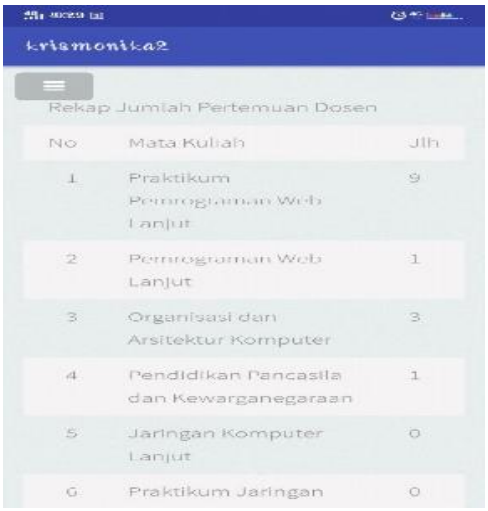
Form Menu Home

Gambar 5. Tampilan Halaman Home

Form Menu FO Monev Dosen

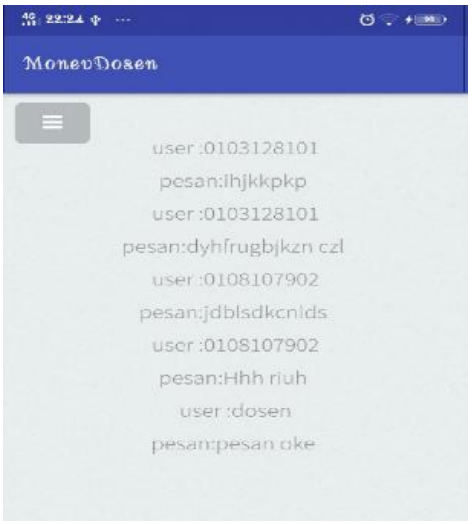
Gambar 6. Tampilan Menu FO Monev Dosen

Tampilan Menu Rekap Pertemuan



Gambar 7. Tampilan Menu Rekap Pertemuan

Tampilan Menu Pesan



Gambar 4.11. Tampilan Menu Pesan

5. KESIMPULAN DAN SARAN

Kesimpulan

1. Sistem monitoring kehadiran dosen dalam proses belajar mengajar tersebut terintegrasi ke Sistem Akademik STMIK-KNI.
2. Sistem tersebut dapat menghitung jam masuk, jam keluar dan keterlambatan dosen yang mengajar.
3. Dosen yang memiliki NIDN yang dapat login kedalam sistem tersebut.

Saran

Dari kesimpulan diatas penulis menemukan beberapa saran yang dapat dijadikan sebagai bahan atau data untuk mempertimbangkan lebih lanjut :

1. Sistem ini dapat dilanjutkan menjadi penilaian kinerja dosen.
2. Agar sistem yang dibangun oleh penulis dapat di aplikasikan di kampus STMIK-KNI sebagai bahan atau alat untuk memonitoring kehadiran dosen dalam kegiatan belajar mengajar.

DAFTAR PUSTAKA

[1]. Akhmad Dharma Kasman. 2015. **Trik Kolaborasi Android dengan PHP & MySQL.** Yogyakarta : Lokomedia.

[2]. Amsler. **Tujuan Sistem Monitoring**. Jurnal Muhammad Revo Dwi Putro, 2014:205

[3]. Kadir.Abdul.2018. **Pemrograman andorid & database**.,Pt Gramedia;Jakarta.

[4]. Mudjahidin. Nyoman Dita Pahang Putra. **Rancang Bangun Sistem Informasi *Monitoring* Perkembangan Proyek Berbasis Web Studi Kasus Dinas Bina Marga dan Pemantusan**. *Jurnal Teknik Industri,* Vol. 11, No. 1, Februari2010: 75-83.

[5]. Muhamad Revo Dwi putro.,dkk. 2014.,**Rancang bangun sistem monitoring antrian pada setia bakti wanita berbasis web**.,Vol 3.,Hal 206. jurnal.stikom.edu/index.php/jsika/article/view/409.

[6]. Romney, Marshall B., dan Paul John Steinbart.2015.**Accounting Information Systems**, 13thed.England: Pearson Educational Limited.

[7]. *Sadeli, Muhammad. 2014.* ***"Aplikasi Bisnis dengan PHP dan MySQL Menggunakan Dreamweaver CS6".*** *Palembang: Maxikom.*

[8]. Silvia, A.F, Haritman, E., Muladi, Y., 2014, **Rancang Bangun Akses Kontrol Pintu Gerbang Berbasis Arduino Dan Android,** Jurnal ELECTRANS, Vol.13, No.1. dokumen.tips/documents/keamanan-ruangan.

[9]. Sutabri Tata, 2016, **Sistem Informasi Manajemen,** Andi Offset, Yogyakarta.

[10].Sujatmiko, Eko.2012. **Kamus Teknologi informasi dan komunikasi.** Surakarta : Aksarra Sinergi Media.

[11]. Wiliam. **Bentuk Sistem Monitoring**. *Jurnal Muhammad Revo Dwi Putro,* 2014:9