Keamanan Transaksi KRSS Online Web Student Universitas Budi Luhur Dengan Algoritma TOTP RFC 6238 Menggunakana Autentikasi SMS

Wahyudi Purnama[1)], **Ferdiansyah**[2)]
Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : wahyudipurnama17@gmail.com[1)], ferdiansyah@budiluhur.ac.id[2)]

Abstrak

Universitas Budi Luhur selalu memfasilitasi dan memotivasi sivitas akademika untuk mencapai penelitian bermutu, salah satunya dengan memberikan pelayanan terhadap mahasiswa/mahasiswi melalui KRSS Online. Dengan ini memudahkan para mahasiswa/mahasiswi dalam membuat rencana studi dan mengurangi beban saat menggunakan metode manual seperti menunggu dan terbuangnya waktu khususnya untuk kelas eksekutif. Namun terdapat kecurangan yang dilakukan seperti melakukan double login ataupun selebihnya yang memberatkan kerja server, melakukan penitipan terhadap teman yang tidak seharusnya diberikan akses dan terjadi repeat process. Untuk menghindari double login untuk user yang sama digunakan session pada halaman web student yang disediakan universitas, sedangkan untuk akses KRSS Online dibuatkan akses TOTP untuk memasukki halaman dengan metode RFC 6238 yang menggabungkan dua metode algoritma yaitu SHA1, Base32 dan satu buah kunci Unixtime untuk menghasilkan angka autentikasi. Angka dikirimkan menggunakan SMS melalui Modem Wavecom M1306B yang terhubung pada komputer dengan aplikasi tambahan yaitu Gammu. Session ini hanya mengijinkan pengguna untuk melakukan akses hanya 1 user dan tidak dapat dilakukan tempat lain, jika dilakukan akan mengeluarkan akses yang dilakukan sebelumnya. TOTP ini hanya dilakukan sekali setelah pengguna melakukan login dan mengakses halaman KRSS Online, hal ini akan berulang kembali jika telah dilakukan logout oleh pengguna. Session TOTP diciptakan agar menghindari autentikasi yang berlebihan dan memakan biaya yang lebih besar. Setelah kode TOTP berhasil dibangkitkan maka akan dikirimkan secara SMS melalui modem Wavecom M1306B dengan kondisi Local Services Windows Gammu SMSD Service sudah diaktifkan, jika tidak pengiriman akan ditunda sampai diaktifkan. TOTP ini memiliki batas waktu atau masa aktif yaitu 5 menit (300 detik) untuk segera dimasukkan karena halaman akan refresh secara otomatis sekaligus menghindari brute force attack, merupakan teknik serangan yang dilakukan terhadap keamanan yang dimiliki komputer dengan melakukan percobaan memasukkan semua kunci yang memiliki pendekatan yang pada awalnya mengacu langsung pada perangkat lunak komputer dan bergantung pada tenaga pemrosesan komputer. TOTP dan Session yang sudah diciptakan akan meningkatkan pelayanan terhadap mahasiswa/mahasiswi Universitas Budi Luhur..

Kata kunci: Gammu, Wavecom M1306B, RFC 6238, Time Based One Time Password, Base32, SHA1, Autentikasi SMS, PHP, HTML, Java, Metode Waterfall

1. PENDAHULUAN

Universitas Budi Luhur sebagai institusi pendidikan tinggi dan penelitian, yang menyediakan pendidikan sarjana dan pascasarjana. Dengan visinya sebagai universitas unggul dengan standar kualitas tertinggi, serta dilandasi kecerdasan dan keluhuran budi, juga ditopang teknologi informasi dan komunikasi. Selalu menyelenggarakan pendidikan berbasik kompetensi agar menghasilkan lulusan yang unggul, cerdas, berbudi luhur, serta mampu bersaing dan kompeten di dunia kerja.

Dalam hal ini universitas selalu memfasilitasi dan memotivasi sivitas akademika untuk mencapai penelitian bermutu salah satunya dengan memberikan pelayanan terhadap mahasiswa atau mahasiswi melalui KRS Online. Dalam meningkatkan kualitas pelayanan Universitas Budi Luhur terhadap mahasiswa/mahasiswi khususnya pada cabang ITC Roxy Mas, diberikan fitur KRSS Online dimana tidak diperlukan lagi kehadiran para mahasiswa/mahasiswi untuk melakukan pengisian Kartu Rencana Studi Sementara (KRSS) secara manual. KRSS Online dibuat bertujuan untuk memudahkan para mahasiswa/mahasiswi dalam membuat rencana studi dan mengurangi beban saat menggunakan metode manual seperti menunggu dan terbuangnya waktu.

Setelah KRSS Online telah berfungsional, ditemukan kendala yang membuat hasil tidak maksimal, seperti kecurangan yang dilakukan mahasiswa seperti dual login dan repeat process yang memberatkan server.

2. METODE PENELITIAN

2.1. Wavecom M1306B

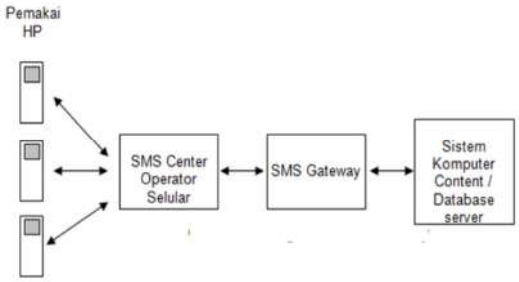
Wavecom merupakan modulator yang berasal dari Perancis. Sebuah perusahaanyang mulai dikenal di negara Indonesia melalui modem Wavecom yang memiliki banyak fungsi. Salah satunya fungsi modem Wavecom merupakan pemberian layanan serta dukungan pada kegiatan industri maupun rumahan untuk SMS Gateway dan lainnya. [1].

2.2. SMS Gateway

SMS gateway merupakan suatu proses mekanisme ataupun sistem pengiriman dan menerima SMS, digunakan dari mobile ataupun

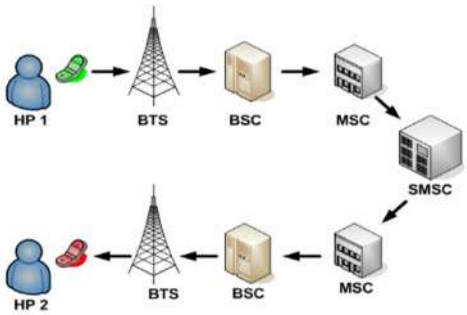
modem SMS seperti wavecom M1306 melalui shortcode yang ada pada SMS Gateway. SMS Gateway adalah sistem aplikasi yang memberikan layanan transit SMS, lalu ditransformasikan pesan menuju jaringan selular dari media lainnya dan memungkinkan bahwa dalam pelaksanaan pengiriman atupun penerimaan pesan SMS ini dapat dilakukan tanpa media seperti ponsel. SMS ini dikirim atau diterima dari SMS Center, merujuk pada content server [2].

a. Diagram SMS Gateway, pengirim mempersiapkan laptop atau PC yang di lengkapi dengan modem yang sudah terisi kartu sim beserta pulsa. SMS Gateway akan menerima pesan dari ponsel dari SMSC lalu diteruskan sebagai input bagi aplikasi yang akan mengakses content tersebut. Data SMS yang dikirim melalui BTS dan berikutnya data pesan singkat disimpan sementara di SMSC lalu dilanjutkan melewati BTS sebelum penerima mendapatkan balasan SMS begitu juga sebaliknya penerima dapat membalas SMS tersebut. Gambaran sederhana sebuah SMS Gateway digambarkan sebagai berikut::



Gambar 1. Diagram SMS Gateway

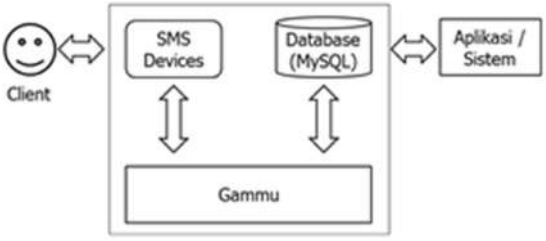
b. Cara Kerja SMS, dapat digambarkan sebagai berikut:



Gambar 2. Cara Kerja SMS

2.3. Gammu

Gammu adalah sebuah aplikasi tambahan yang dapat dipasang dan beroperasi di latar belakang dan dapat dinyalakan setelah modem telah tersambung dan pengaturan sudah sesuai. Digunakan juga sebagaijembatan media untuk komunikasi pada database dengan sms devices. Gammu diciptakan oleh Michar Cihar yang merupakan seorang programmer python asal Jerman. Cihar juga telah menciptakan beberapa library yang berfungsi serta bertujuan untuk manajemen pada ponsel. Menurut Cihar (2015), gammu sebuah aplikasi jembatan komunikasi yang dapat digunakan pada berbagai handphone, modem dan perangkat sejenis lainnya. Gammu juga memiliki kemampuan sebagai media untuk memonitor sms devices beserta database sms gateway, saat sms masuk ke sms devices maka gammu langsung memasukan pada database dengan table inbox. Sedangkan untuk pengiriman gammu akan memproses yang ada pada table outbox setelah berhasil terproses akan dipindahkan secara otomatis pada table sentItems melalui smsdevices [3].



Gambar 3. Proses Gammu

2.4. SHA1

Secure Hash Algorithm (SHA) merupakan fungsi hash dengan satu arah, dibuat dan didesain oleh National Security Agency lalu diumumkan oleh NIST (National Institute of Standard and Technology). Terdapat banyak versi SHA yakni SHA-0, SHA-1, SHA-2 dan SHA-2 ini terbagi banyak. SHA dikatakan aman karena dirancang sehingga dengan cara komputasi tidak mungkin untuk menemukan string yang sesuai dengan message digest yang diberikan [4].

SHA-1 merupakan proses mendapat masukan yang bertipe string dan ukuran maksimal 264 bit. Pada setiap string, SHA-1 akan memberikan hasil sebanyak 160 bit dari string tersebut yang biasa juga disebut message digest. Panjang jarak sebuah message digest ini bisa berkisar antara 160-512 bit berdasarkan algoritmanya. Berdasarkan sifatnya SHA-1, dapat digunakan dengan algoritma kriptografi lainnya seperti pada Diginal Singature Algorithms (biasa digunakan) atau dalam generasi angka yang diacak (bits). SHA-1 diperhitungkan aman dikarenakan dihitung secara tidak terlihat untuk mencari string yang sesuai untuk memperoleh sebuah message digestnya atau dapat juga digunakan untuk mencari dua string yang berbeda untuk dihasilkan message digest yang sama.

Pada SHA-1 memiliki ukuran blok string (m bit) yang ditentukan berdasarkan algoritmanya. Pada SHA-1 masing-masing pada blokstring memiliki 512 bit dimana akan dilakukan dengan 16 urutan dan

ukuran sebesar 32 bit. SHA-1 ini akan digunakan sebagai media untuk menghitung message digest pada string input dengan tujuan memperoleh string ini diisi sebagai perkalian dari 512 bits. Hal-hal yang dilakukan dalam mengisi string:

a. Panjang dari string, M merupakan k bits dimana panjangnya k < 264. Tambahkan bit "1" pada akhir string. Misalkan string yang asli adalah "01010000" maka setelah diisi menjadi "010100001".
b. Ditambahkan bit "0", angka bit "0" berdasarkan dari panjang string. Misalnya: String aslinya adalah bit string: abcde
   01100001 01100010 01100011 01100100 01100101.

   Setelah proses (a) dilakukan hasilnya:
   01100001 01100010 01100011 01100100 01100101.

   Panjang k = 40 dan angka bit yang sudah diproses adalah 41 dan 407 lalu ditambahkan bit "0" (448 – (40+1) =407). Kemudian diubah menjadi sebuah hex:
   61626364 65800000 00000000 00000000
   00000000 00000000 00000000 00000000
   00000000 00000000 00000000 00000000
   00000000 00000000
c. Untuk mendapatkan hasil 2 kata dari k, angka bit dalam string asli yaitu jika k < 2
   32 artinya kata pertama adalah semua bit dengan nilai "0". Maka gambaran akhir 2 kata dari k = 40 dalam nilai hexnya:
   00000000 00000028.
   61626364 65800000 00000000 00000000
   00000000 00000000 00000000 00000000
   00000000 00000000 00000000 00000000
   00000000 00000000 00000000 00000028

SHA-1 ini menggunakan sebuah fungsi logika yang digambarkan dengan f0,f1 sampai f79. Untuk masing=masing ft, dimana kondisinya $0 \leq t < 79$ memberikan hasil output sebanyak 32 bit dan berikut adalah fungsinya:

$$f_t(B,C,D) = \begin{cases} (B \wedge C) \vee (\neg B \wedge D) & 0 \leq t \leq 19 \\ B \oplus C \oplus D & 20 \leq t \leq 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & 40 \leq t \leq 59 \\ B \oplus C \oplus D & 60 \leq t \leq 79 \end{cases}$$

⊕ = fungsi XOR

Gambar 4. Step 1 SHA1

Konstanta kata yang dipakai dalam SHA-1 disimbolkan secara terurut dimulai dari K(0), K(1) sampai K(79) dalam bentuk nilai hex sepert pada fungsi 02 berikut:

$$K_t = \begin{cases} 5A827999 & 0 \leq t \leq 19 \\ 6ED9EBA1 & 20 \leq t \leq 39 \\ 8F1BBCDC & 40 \leq t \leq 59 \\ CA62C1D6 & 60 \leq t \leq 79 \end{cases}$$

Gambar 5. Step 2 SHA1

2.5. Base32

Base32 merupakan notasi untuk pengkodean data byte menggunakan seperangkat terbatas simbol yang dapat dengan mudah digunakan oleh user dan diproses oleh sistem komputer yang hanya mengenali rangkaian karakter dibatasi. Ini terdiri dari simbol set terdiri dari 32 karakter yang berbeda, serta algoritma untuk encoding string menggunakan 8-bit karakter ke dalam alfabet Base32. Ini menggunakan lebih dari satu 5-bit Base32 simbol untuk setiap karakter masukan 8-bit, dan dengan demikian juga menentukan persyaratan pada panjang diperbolehkan dari Base32 string (yang harus kelipatan dari 40 bit)[5]. Urutan kerja Base32 adalah sebagai berikut :

a. Ubah text ke kode ASCII
b. Kode ASCII di convert ke BINER 8 Bit
c. Hasil BINER 8 bit dibagi menjadi 5 bit per blok
d. Bit pattern per blok akan di konvesi kembali ke decimal
e. Hasil dari decimal akan di dicocokkan ke tabel index base32

Table 1. Tabel Base32

Value	Symbol	Value	Symbol	Value	Symbol
0	A	14	O	28	4
1	B	15	P	29	5
2	C	16	W	30	6
3	D	17	R	31	7
4	E	18	S	*pad*	=
5	F	19	T		
6	G	20	U		
7	H	21	V		
8	I	22	W		
9	J	23	X		
10	K	24	Y		
11	L	25	Z		
12	M	26	2		
13	N	27	3		

2.6. RFC (Request For Comment) 6238

RFC 6238 merupakan variasi dari algoritma HOTP menentukan perhitungan dari nilai password

satu kali, berdasarkan representasi dari counter sebagai faktor waktu. RFC 6238 merupakan pengembangan dari RFC 4226 yang dibuat oleh M'Raihi, et al. RFC 6238 ini diimplementasikan sebagai berikut:

a. Buat sebuah kunci, K, yang merupakan string byte yang hanya dibagikan secara aman kepada klien.
b. Setuju pada T0, dimana waktu Unix untuk mulai menghitung langkah waktu dari dan interval TI, yang akan digunakan untuk menghitung nilai counter C.
c. Menggunakan Cryptographic Hash Method SHA-1.
d. Jumlah nilai token yang digunakan 6.

Meskipun RFC 6238 memungkinkan parameter yang berbeda untuk digunakan, penerapan yang dilakukan oleh google terhadap aplikasi autentikasi ini tidak mendukung T0, nilai T1, metode hash dan panjang token yang berbeda dari standar. Ini juga memberikan ekspetasi terhadap kunci rahasia K untuk dimasukkan (atau disertakan dalam kode QR) dalam pengkodean base-32 sesuai dengan RFC 3548[6].

3. METODE PENELITIAN

3.1. Metode Penelitian

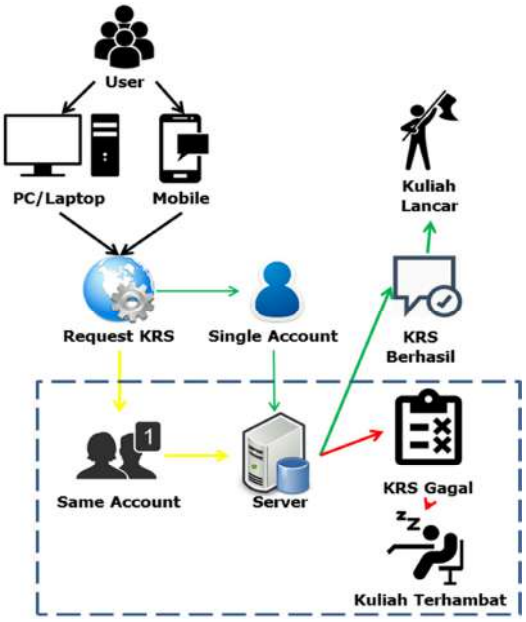
Metode pengembangan yang kami lakukan menggunakan metode waterfall dengan tahap-tahap sebagai berikut:

a. Analisis, Beberapa hal yang dilakukan dalam membuat analisa untuk menunjang penelitian ini diantaranya dengan melakukan wawancara dengan mahasiswa/mahasiswi Universitas Budi Luhur.
b. Desain, Setelah dilakukan analisa, dibuat desain rancangan sistem menggunakan use case, flowchart, algoritma dan rancangan layar sebagai dasar pembuatan tampilan layar dan alur kerja dari aplikasi, agar mempermudah proses pengkodean.
c. Pengkodean, Tahap pengkodean dilakukan setelah desain selesai dirancang. Untuk mengimplementasikan design rancangan layar menjadi tampilan form, mengunakan bahasa pemograman PHP 5.6.31 digabungkan dengan gammu untuk meningkatkan kualitas program, setelah tampilan form jadi, maka sebagai pemrosesan data-data yang nantinya akan saling terhubung atau berhubungan dengan database MySql sebagai database penyimpanan data.
d. Pengujian, Tahapan selanjutnya setelah menyelesaikan pembuatan desain dan bahasa pemogramannya maka dilakukan tahap pengujian menggunakan Notepad++, Mozilla Firefox dan Google Chrome. Jika masih ada beberapa hal yang masih belum berjalan lancar maka dilakukan perbaikan dengan memperbaiki dibagian yang belum berjalan lancar misalkan dibagian pemogramannya maupun rancangan layar.

3.2. Analisa Masalah

Berdasarkan hasil observasi dan wawancara yang dilakukan oleh penulis pada mahasiswa/i Universitas Budi Luhur Roxy, Kampus-B Roxy. Di dalam melakukan proses pendaftaran SKS melalui KRSS Online barang pada student.budiluhur.ac.id masih tidak optimal. Sehingga proses pendaftaran yang memakan waktu yang cukup lama, para mahasiswa/i khususnya cabang Roxy memiliki 2 fakultas yaitu fakultas teknologi informasi, fakultas ekonomi dan bisnis.

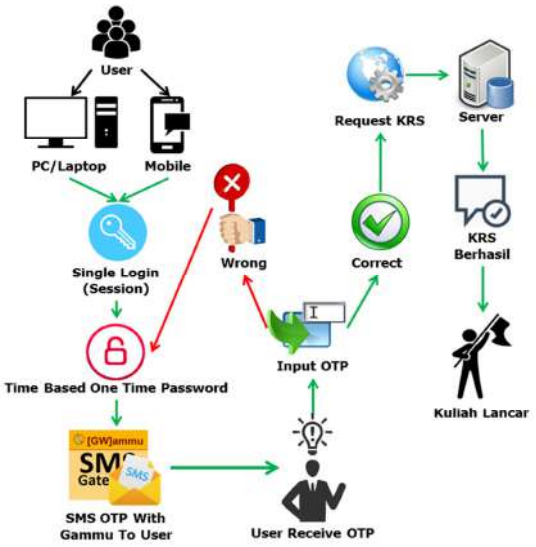
Kedua fakultas ini merupakan fakultas yang besar dan jumlahnya selalu bertambah setiap semesternya, namun masalah terhadap pendaftaran melalui KRSS Online ini memberikan hambatan yang membuat para mahasiswa/i kecewa dengan pelayanan. Berdasarkan analisa masalah yang ada penulis mencoba untuk menciptakan inovasi baru dimana inovasi ini di jadikan solusi dari permasalah yang ada yaitu dengan membuat sebuah teknologi tambahan pada KRSS Online.



Gambar 6. Masalah Sekarang

3.3. Solusi Masalah

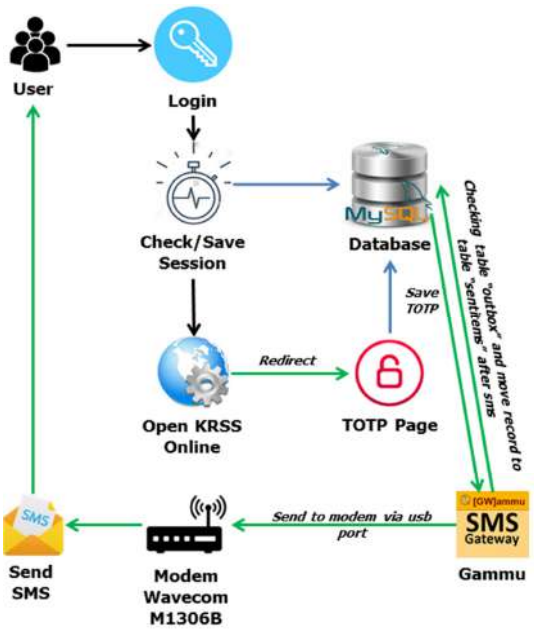
Berdasarkan analisa masalah yang ditemukan, berikut solusi rancangan yang dibuat:



Gambar 7. Rancangan Solusi Masalah

3.4. Rancangan Kerja Alat dan User

Berdasarkan solusi masalah yang dibuat, berikut rancangan kerja alat dan user yang dibuat:



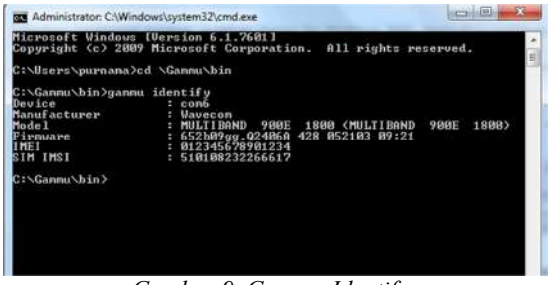
Gambar 8. Rancangan Kerja Alat Dan User

4. HASIL DAN PEMBAHASAN

Naskah dikirim melalui email dalam format Word. Paper dikirimkan sebelum pendaftaran TA berakhir.

4.1. Prosedur Operasional

Melakukan percobaan verifikasi koneksi komputer dengan gammu beserta modem yang sudah dipasang.



Gambar 9. Gammu Identify

Setelah sudah, maka dilakukan *install* pada *windows services* dengan perintah *command prompt* gammu-smsd –c smsdr –i dan dapat menjalankan services dengan perintah gammu-smsd-c smsdrc -s.

4.2. Implementasi Aplikasi

Pengujian sistem ini bertujuan untuk mengetahui seberapa efektif dan akurat OTP yang dikirimkan melalui modem wavecom m1306b. Pada ujicoba simulasi untuk mengetahui apakah sistem dapat bekerja dengan baik atau tidak, dan hasilnya apakah sudah sesuai dengan keinginan atau masih perlu dilakukan perbaikan. Hal-hal tersebut akan diketahui jika sudah dilakukan simulasi ujicoba sistem.

Gambar 10: Tampilan Halaman Utama

Jika password yang dimasukkan salah maka akan tampil sebuah notifikasi seperti gambar berikut.

Gambar 11. Notifikasi NIM/Password Salah

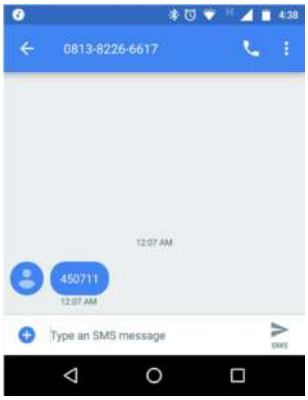
Setelah halaman utama muncul, dapat melakukan login ataupun pendaftaran mahasiswa. Disini kita akan melakukan login, berhasil dan tampilan berubah menjadi seperti gambar berikut.

Gambar 12. Tampilan Menu Utama

Setelah menu utama muncul, maka kita akan memilih menu KRSS Online. Jika belum pernah melakukan OTP maka halaman akan dialihkan ke Input OTP.

Gambar 13. Tampilan OTP

Bukti bahwa SMS telah diterima dengan baik :



Gambar 14. Terima Kode OTP

Jika OTP berhasil dimasukkan, maka mahasiswa sudah dapat mengakses transaksi halaman KRSS Online. Disini mahasiswa akan memilih periode untuk melakukan pengisian rencana studi kuliah mereka pada semester depan.

Gambar 15. Tampilan KRSS Online

Hasil pengujian dari aplikasi yang sudah dibuat sebagai berikut:

Table 2. Tabel Pengujian Aplikasi Dan Modem

No	Tombol	Ekspetasi	Hasil	
			Bisa	Keterangan
1	Login	Melakukan login	☑	Berhasil
2	Daftar	Melakukan daftar mahasiswa	☑	Berhasil
3	Session	Hanya dapat melakukan single login	☑	Berhasil
4	OTP	Menghasilkan digit OTP untuk dikirim	☑	Berhasil
5	Database	Terkoneksi dengan program	☑	Berhasil
		Dapat menyimpan	☑	Berhasil
6	SMS	Dapat mengirimkan OTP (Service Aktif)	☑	Berhasil
		Dapat mengirimkan OTP (Service NonAktif)	☐	Gagal
7	Modem Waveco m M1306	Terhubung dengan komputer	☑	Berhasil
		Local Services dapat dijalankan	☑	Berhasil

4.3. Evaluasi Hasil Uji Coba Sistem

Evaluasi ini bertujuan untuk menganalisa hasil ujicoba sistem yang telah dirancang. Sistem ini tentu mempunya kekurangan dan kelebihan tersendiri jika ditinjau dari kebutuhan penggunaan yang beragam dengan kondisi dan situasi berbeda-beda.

a. Kelebihan Sistem, Beberapa hal yang menjadi kelebihan dari sistem OTP dengan autentikasi SMS yang penulis rancangan antara lain :
   (1) Single Session yang dibuat pada sistem berjalan dengan baik.
   (2) Database dapat terkoneksi dengan program, dapat menyimpan.
   (3) Program dapat melakukan pengiriman pesan sebagai media autentikasi.

(4) Proses menghasilkan angka OTP berjalan dengan baik dengan metode RFC6238.
(5) Modem Wavecom M1306B dapat terhubung dengan komputer, program dapat mendeteksi modem melalui koneksi serial port sekaligus gammu yang terhubung untuk menghubungkan dengan komputer.

b. Kekurangan Sistem, Karena keterbatasan sumber daya dan waktu untuk riset secara mendalam, dalam pengembangan sistem aplikasi OTP dengan autentikasi SMS ini masih ditemui beberapa kekurangan dan kelemahan diantaranya:
(1) Pengiriman pesan hanya dapat dijalankan jika local service Gammu telah dinyalakan.
(2) Belum terdapat fitur jika pengiriman pesan gagal dikirimkan untuk diinformasikan kepada mahasiswa/mahasiswi.
(3) Koneksi serial port untuk modem diatur secara absolute tidak dapat relative.

5. KESIMPULAN

Berdasarkan evaluasi hasil pengujian perangkat OTP dan modem Wavecom M1306B ini maka penulis membuat kesimpulan :

a. Modem dapat digunakan sebagai pengirim pesan dan meningkatkan kualitas pelayanan dari segi keamanan. Metode OTP juga memberikan umpan timbal balik yang lebih baik sehingga tidak sembarangan yang dapat melakukan akses KRSS Online.
b. Single Session Login yang dibuat dapat mengurangi kecurangan seperti dual login yang memberikan kinerja lebih banyak terhadap server dan merugikan mahasiswa/mahasisiwi lain yang akan menggunakan KRSS Online.

6. DAFTAR PUSTAKA

[1] Daswanto, Aldi. 2016. Wavecom. Available at : https://www.beli.com/mengenal-lebih-dekat-modem-wavecom-dan-layanan-sms-gateway/ [Diakses pada Oktober 17, 2017].
[2] Suryana, Taryana. 2012. SMS Gateway Kannel Sebagai Sarana Penunjang Informasi Akademik. Bandung. Jurnal Ilmiah Komputer dan Informatika (KOMPUTA).
[3] Micharl Cihar. 2016. Gammu. Available at : https://wammu.eu/docs/pdf/gammu.pdf [Diakses pada Oktober 17, 2017].
[4] Aryasa, Komang & Paulus, Yesaya Tommy. 2013. Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pemprograman Java. Yogyakarta. Citec Journal.
[5] Riza Ardian, Ferino. 2013. Implementasi Encoding Algoritma Base16, Base32dan Base 64 Untuk Teks. Medan. Universitas Sumatera Utara.
[6] M'Raihi, David, Machani, Salah, Pei, Mingliang, Rydell, Johan. Request For Customer 6238. USA. Internet Engineering Task Force (IETF).