

## **BAB IV**

### **HASIL DAN PEMBAHASAN**

#### **4.1 Hasil Implementasi Sistem**

Perancangan sistem dibuat menggunakan bahasa PHP, Python, dan protokol LDAP dengan *Microsoft Active Directory* sebagai basis data penggunaannya. Pada bab ini penulis akan menjelaskan tentang implementasi sistem dari perancangan yang telah dibuat pada bab sebelumnya. Penulis akan menjelaskan fungsi dari masing-masing *stackholder* yaitu pengguna umum (civitas akademik UII), pegawai akademik dan pegawai keamanan (security) ketika menggunakan sistem. Pembagian hak akses dari semua *stackholder* dilakukan dengan cara membuat sebuah group pada basis data LDAP yang terdiri dari group xirka (pengguna umum/civitas akademik), group akademik (pegawai akademik), dan group keamanan (pegawai keamanan). Pada bab ini juga akan dijelaskan proses bisnis yang diterapkan ketika pengguna akan meminta akses ke sebuah ruangan.

##### **4.1.1 Proses Bisnis Pengajuan Akses Ruangan**

Pada bagian ini, penulis akan menjelaskan secara garis besar yang akan meliputi semua *stackholder* terkait (civitas akademik, pegawai akademik, dan pegawai keamanan) ketika akan menggunakan aplikasi ini. Skenario yang digunakan adalah proses bisnis ketika pengguna ingin meminta akses ke sebuah ruangan sampai pengguna tersebut berhasil mendapatkan akses ruangan yang diinginkan. Adapun langkah-langkah yang dilakukan adalah sebagai berikut:

1. Pengguna (civitas akademik UII) datang ke Direktorat Layanan Akademik, Universitas Islam Indonesia dengan membawa kartu identitas yang dimiliki untuk dilakukan asosiasi kartu ke dalam basis data.
2. Petugas akademik melihat kartu identitas pengguna dan melakukan tap kartu ke reader serta memasukkan data nomor induk ke aplikasi web untuk diproses.
3. Setelah berhasil melakukan asosiasi kartu ke dalam basis data, pengguna melakukan login ke web aplikasi untuk membuat permintaan akses

ruangan dan mencetak suratnya (bisa dalam bentuk file/hardcopy). Surat tersebut lalu ditunjukkan/dibawa ke Unit Satuan Pengamanan Gedung, Universitas Islam Indonesia.

4. Pegawai security lalu membaca daftar ruangan yang diminta oleh pengguna melalui surat tersebut untuk melakukan validasi bahwa pengguna tersebut adalah benar-benar civitas akademik UII. Setelah itu pegawai security memberikan akses sesuai dengan daftar ruangan yang diminta oleh pengguna.
5. Pengguna berhasil mendapat akses ruangan yang diminta.

Proses bisnis pengajuan akses ruangan digambarkan pada Gambar 4.1 berikut:



Gambar 4.1 Proses Bisnis Pengajuan Akses Ruangan

#### 4.1.2 Proses Bisnis Blokir Akses Ruangan (Kehilangan Kartu)

Blokir akses ruangan dapat dilakukan jika pengguna mengalami kehilangan kartu. Blokir akses ruangan dilakukan agar akses ruangan yang telah diberikan pada kartu yang lama (kartu yang hilang) tidak disalahgunakan oleh pihak yang menemukan kartu tersebut. Blokir akses ruangan merupakan salah satu syarat untuk membuat kartu yang baru dan mendapatkan kembali akses ruangan yang pernah

diberikan sebelumnya. Adapun langkah-langkah yang dilakukan untuk melakukan blokir akses ruangan dan mendapatkan kembali akses ruangan dengan membuat kartu baru adalah sebagai berikut:

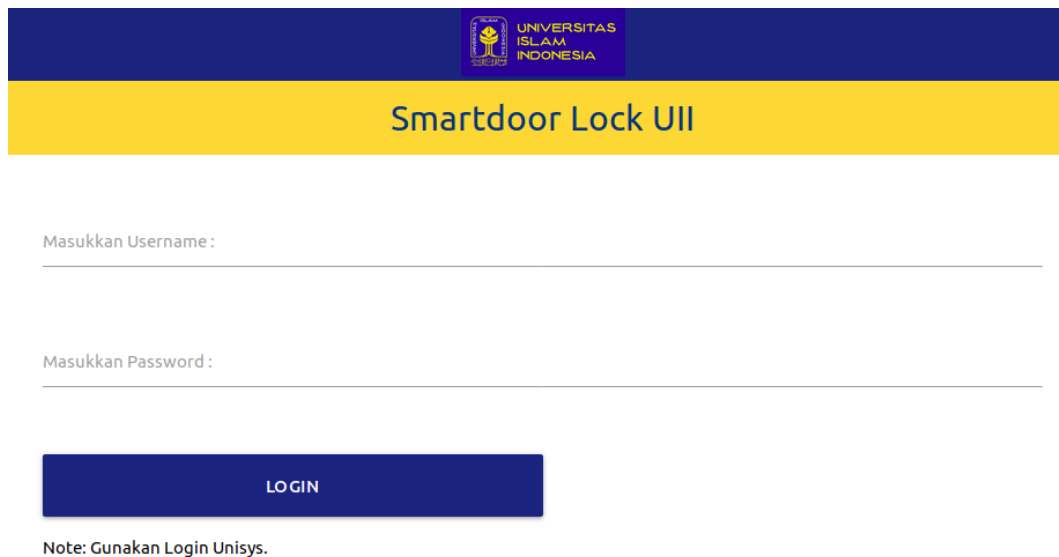
1. Pengguna yang mengalami kehilangan kartu melapor ke Direktorat Layanan Akademik untuk dilakukan blokir akses ruangan.
2. Petugas Akademik memblokir akses ruangan pengguna, lalu membuat kartu identitas yang baru.
3. Setelah kartu identitas yang baru selesai dibuat, pengguna meminta petugas akademik untuk melakukan asosiasi kartu ke dalam basis data kembali.
4. Setelah kartu berhasil diasosiasikan ke dalam basis data, pengguna melapor ke bagian keamanan (security) untuk meminta akses ruangan kembali seperti yang pernah diberikan sebelumnya dengan menunjukkan kartu identitas yang baru.
5. Pengguna berhasil mendapat akses ruangan yang diminta seperti kembali seperti sebelumnya.

#### 4.1.3 Login Aplikasi

Aplikasi *backend* yang digunakan untuk akses kontrol ruang yaitu berbasis web dimana memiliki satu halaman yang digunakan untuk login pengguna ke dalam aplikasi ini. Semua *stackholder* (civitas akademik, pegawai akademik, dan pegawai keamanan) melakukan login melalui halaman yang sama. Semua *stackholder* sudah memiliki *role* masing-masing yang diatur di dalam basis data *Microsoft Active Directory* menggunakan protokol LDAP. Jadi pengguna tidak perlu lagi membuat akun baru untuk menggunakan aplikasi ini, pengguna cukup menggunakan akun Unisys yang telah dimiliki oleh setiap civitas akademik di UII.

Satu hal yang perlu diperhatikan adalah pengguna hanya bisa melakukan login ketika sudah melakukan asosiasi kartu ke bagian akademik, terkecuali pegawai akademik dan pegawai security dimana akses login diatur oleh pihak tertentu melalui pengaturan di basis data LDAP atau Microsoft Active Directory

UII. Berikut adalah tampilan form login dari aplikasi *backend* akses kontrol ruangan yang ditunjukkan pada Gambar 4.2:



Masukkan Username :

Masukkan Password :

LOGIN

Note: Gunakan Login Unisys.

Gambar 4.2 Form Login Aplikasi Akses Kontrol Ruang

#### 4.1.4 Pengguna Umum (Civitas Akademik)

Pengguna umum atau civitas akademik UII memiliki peran sebagai pengguna yang akan menggunakan dan mendapatkan akses ruangan tertentu. Pegawai akademik dan pegawai keamanan juga bisa bertindak sebagai pengguna umum apabila ingin mendapatkan akses ruangan tertentu. Oleh karena itu pengguna umum harus melakukan pengajuan akses ruangan dengan membuat daftar permintaan akses ruangan di aplikasi web yang telah disediakan seperti yang ditunjukkan pada Gambar 4.3.



Gambar 4.3 Membuat Permintaan Akses Ruangan

Setelah membuat daftar permintaan akses ruangan, pengguna dapat melihat daftar permintaan ruangan yang telah dibuat. Disana terdapat detail kode ruang, nama ruang, tanggal pembuatan dan status apakah ruangan yang diminta telah disetujui atau belum seperti yang ditunjukkan pada Gambar 4.4.



No	Nama	NIM/NIK	Kode Ruang	Nama Ruang	Update	Status
1	Bayu Aprilananda Sujatmoko	15523090	523	Lab Teknik Informatika	2019-08-14 07:48:50	Disetujui

Gambar 4.4 Daftar Permintaan Akses Ruangan

Langkah selanjutnya setelah melihat daftar permintaan akses ruangan, pengguna diharuskan untuk menekan tombol “Cetak Surat Pengajuan Akses

Ruangan” agar daftar permintaan akses ruangan dapat dilihat oleh pegawai keamanan untuk dilakukan validasi. Pengguna juga boleh membawa *print out* surat pengajuan akses ruangan tersebut dan memberikannya kepada pegawai keamanan untuk diverifikasi seperti yang terlihat pada Gambar 4.5.

**Surat Pengajuan Akses Ruangan**  
Nomor Surat : 39/15523090/REQ/ACC/RG/UII/13-07-2019

Civitas akademik Universitas Islam Indonesia yang bernama Bayu Aprilananda Sujatmoko dengan nomor induk 15523090, mengajukan permintaan akses ruangan pada tanggal 13 Juli 2019 agar dapat menggunakan ruangan yang terdapat pada daftar sebagai berikut:

Kode Ruang	Nama Ruang
523	Lab Teknik Informatika
524	Lab Teknik Elektro

Demikian surat ini dibuat, agar dapat dipergunakan sebagaimana mestinya.


Yogyakarta, 13 Juli 2019  
Yang Mengajukan Akses Ruangan

Petugas Keamanan UII

NIK. \_\_\_\_\_ Nomor Induk. \_\_\_\_\_

Gambar 4.5 Surat Pengajuan Akses Ruangan

Setelah pengguna mendapatkan akses ruangan yang diinginkan, pengguna dapat melihat daftar ruangan yang bisa diakses melalui halaman “Daftar Akses Ruangan”. Disana terdapat detail informasi dari setiap pengguna meliputi data diri pengguna seperti *uid card*, nama, nomor induk, jurusan, email dan daftar ruangan seperti yang ditunjukkan pada Gambar 4.6.



Info Update Kartu	2019-08-16 12:56:18   kartu_sudah_diasosiasikan
ID Card	a06f16be
Username	15523090
Nama Lengkap	Bayu Aprilananda Sujatmoko
Nama Belakang	Sujatmoko
Email	bayusujatmoko@gmail.com
Email	bayusujatmoko@yahoo.com
Akses Ruangan	REK-DL-LT4-01 - Ruang Sekretariat BSI UII
Akses Ruangan	523 - Lab Teknik Informatika

Gambar 4.6 Daftar Akses Ruangan

#### 4.1.5 Pegawai Akademik

Pegawai akademik memiliki peran untuk melakukan asosiasi kartu identitas setiap pengguna civitas akademik UII ke dalam basis data Microsoft Active Directory yang berbasis LDAP. Pegawai melakukan tap kartu ke RFID reader dan memasukkan nomor induk pengguna ke dalam form untuk di submit ke basis data. Data yang dikirimkan adalah *uid card* dari kartu setiap pengguna yang disimpan pada atribut “employee number” di entri akun pengguna. Selain melakukan asosiasi, sistem secara otomatis akan menempatkan nomor induk setiap pengguna pada group “xirka” dimana semua pengguna yang akan mendapatkan akses untuk menggunakan ruangan melalui otentikasi RFID reader akan dimasukkan ke dalam group ini. Hal ini bertujuan untuk melakukan validasi bahwa pengguna benar-benar civitas akademik UII yang akan mendapatkan akses untuk menggunakan aplikasi web tersebut.

Pegawai akademik juga bisa bertindak sebagai pengguna umum yaitu pengguna yang akan meminta dan mendapatkan akses ruangan tertentu melalui tab

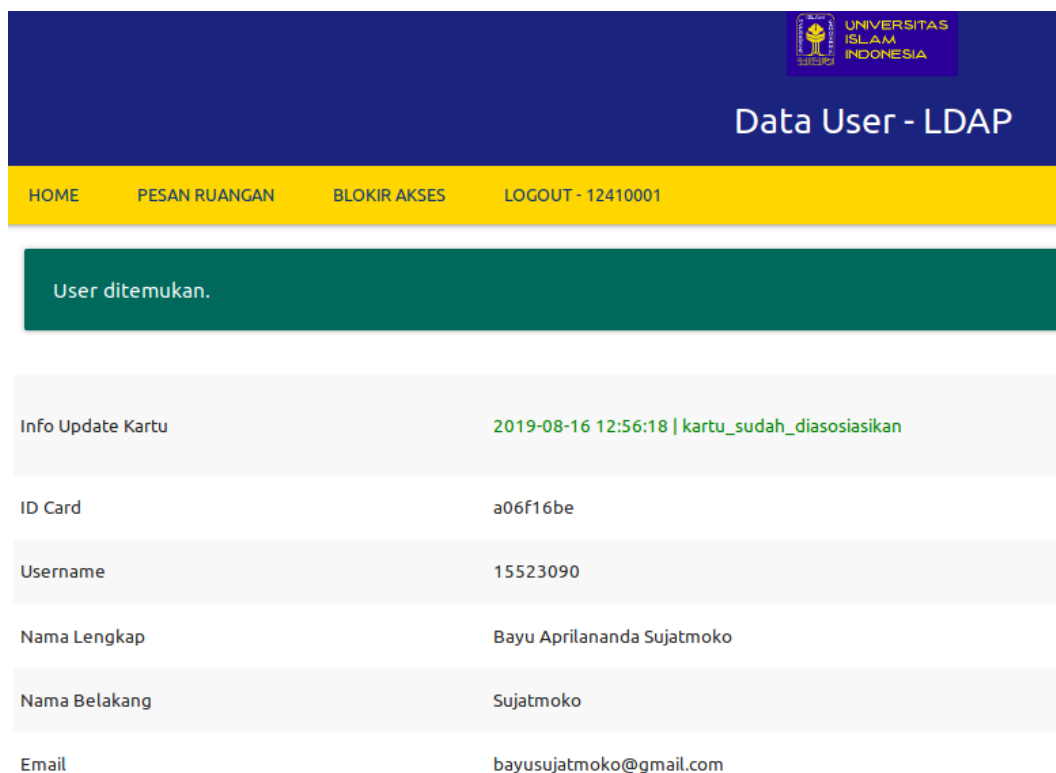
navigasi pesan ruang. Untuk prosedur pengajuan akses ruangan sama seperti yang telah dijabarkan sebelumnya. Form asosiasi kartu pengguna akan ditunjukkan pada Gambar 4.7.

The screenshot shows a web interface for associating a card with an LDAP account. The top navigation bar is dark blue, featuring the Universitas Islam Indonesia logo and the text 'Asosiasi Kartu - LDAP'. Below this is a yellow bar with 'PESAN RUANGAN' and 'LOGOUT - 12410001'. The main content area is white, titled 'Form Asosiasi Kartu dengan Akun LDAP'. It includes the instruction 'Arahkan Cursor ke "Field ID Card" lalu tap kartu ke USB RFID Reader', a 'Field ID Card' input field, a 'Masukkan NIM/NIK' input field, and a dark blue button labeled 'ASOSIASIKAN KARTU'.

Gambar 4.7 Form Asosiasi Kartu Pengguna ke Basis Data LDAP

Setelah melakukan asosiasi kartu pengguna ke basis data LDAP, pegawai akademik dapat melihat beberapa detail mengenai informasi pengguna seperti nama, nomor induk, email dan uid card yang telah berhasil diasosiasikan ke dalam basis data. Pada halaman tersebut pegawai akademik dapat melihat pesan telah berhasil melakukan asosiasi kartu pengguna begitu juga sebaliknya yang ditunjukkan pada Gambar 4.8.





Data User - LDAP	
Info Update Kartu	2019-08-16 12:56:18   kartu_sudah_diasosiasikan
ID Card	a06f16be
Username	15523090
Nama Lengkap	Bayu Aprilananda Sujatmoko
Nama Belakang	Sujatmoko
Email	bayusujatmoko@gmail.com

Gambar 4.8 Halaman Verifikasi Asosiasi Kartu Pengguna ke Basis Data LDAP

Selain melakukan asosiasi kartu, petugas akademik memiliki peran untuk melakukan blokir akses ruangan pengguna jika pengguna tersebut mengalami kehilangan kartu. Hal ini dilakukan agar kartu pengguna yang hilang tersebut tidak disalahgunakan oleh pihak yang menemukan kartu tersebut. Kartu yang hilang tersebut tentunya sudah memiliki beberapa akses terhadap ruang tertentu di UII dan jika sampai digunakan oleh yang bukan pemilik kartu aslinya maka orang tersebut dapat memasuki ruangan yang telah diberikan aksesnya ke kartu yang hilang tersebut. Tentunya hal ini akan sangat beresiko dari sisi keamanan, karena kemungkinan orang asing dapat mengakses ruangan dengan akses terbatas di UII. Petugas akademik hanya perlu memasukkan data nomor induk pengguna untuk melakukan proses blokir akses ruangan.

Oleh karena itu, mekanisme blokir akses ruangan dilakukan sebelum pengguna membuat kartu identitas yang baru di Direktorat Layanan Akademik agar akses ruangan pada kartu dan asosiasi kartu dengan kartu yang lama dihapus sepenuhnya. Setelah asosiasi kartu dan akses ruangan pada kartu yang lama

dihapus, pengguna dapat membuat kartu identitas yang baru di Direktorat Layanan Akademik, melakukan asosiasi kartu yang baru ke basis data LDAP, dan melapor kembali ke bagian keamanan agar diberikan akses ruangan kembali seperti yang pernah diberikan sebelumnya pada kartu yang lama. Berikut adalah halaman form untuk melakukan proses blokir akses ruangan dan menampilkan data pengguna bahwa kartu pengguna tersebut sudah tidak diasosiasikan ke dalam basis data yang digambarkan pada Gambar 4.9 dan Gambar 4.10.



UNIVERSITAS ISLAM INDONESIA

### Blokir Akses Ruangan (Kehilangan Kartu)

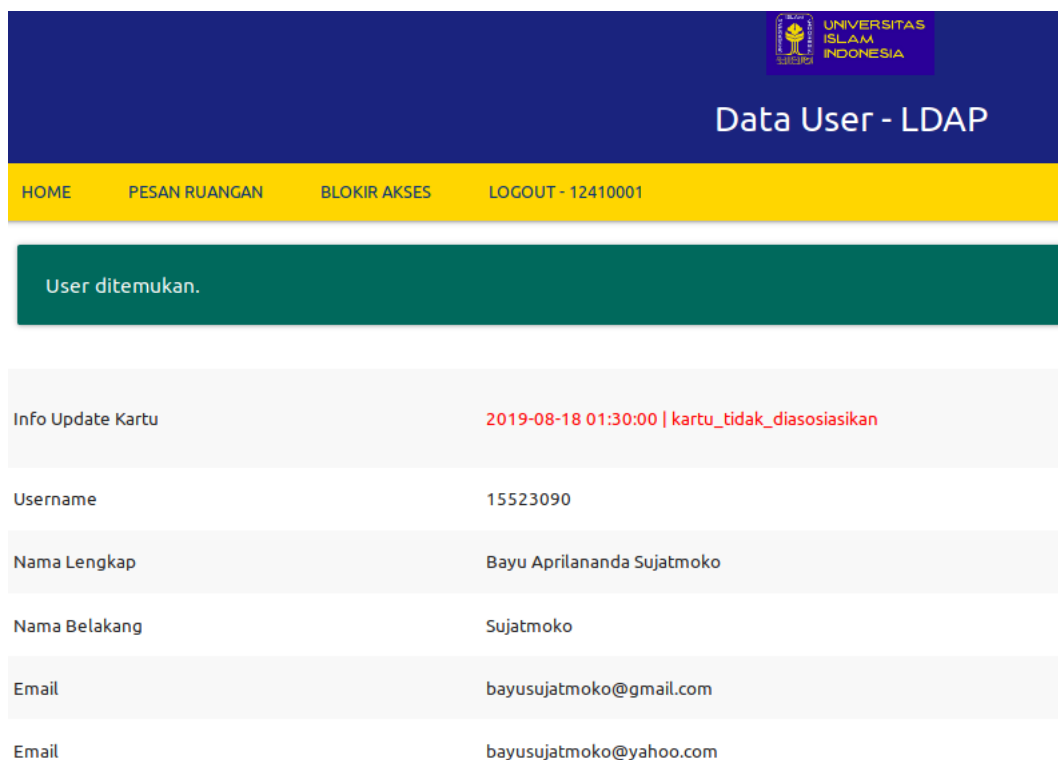
HOME PESAN RUANGAN BLOKIR AKSES LOGOUT - 12410001

Form Blokir Akses Ruangan Pengguna (Kehilangan Kartu)

Masukkan NIM/NIK:

SUBMIT

Gambar 4.9 Form Blokir Akses Ruangan Pengguna



UNIVERSITAS ISLAM INDONESIA

## Data User - LDAP

HOME PESAN RUANGAN BLOKIR AKSES LOGOUT - 12410001

User ditemukan.

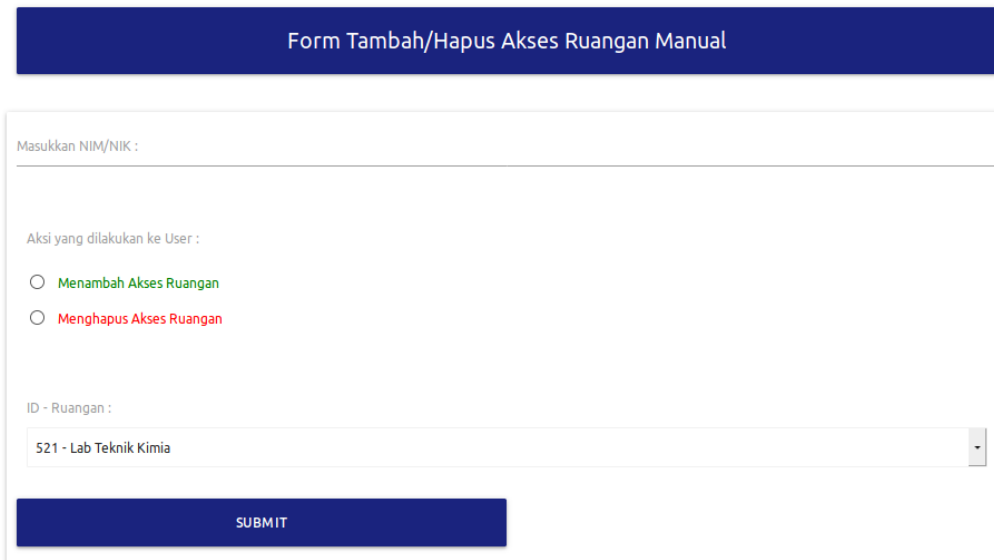
Info Update Kartu	2019-08-18 01:30:00   kartu_tidak_diasosiasikan
Username	15523090
Nama Lengkap	Bayu Aprilananda Sujatmoko
Nama Belakang	Sujatmoko
Email	bayusujatmoko@gmail.com
Email	bayusujatmoko@yahoo.com

Gambar 4.10 Halaman Detail Pengguna Mengenai Info Kartu (Tidak Diasosiasikan)

#### 4.1.6 Pegawai Keamanan (Security)

Pegawai keamanan (security) merupakan *stackholder* yang memiliki peranan yang cukup penting karena pemberian akses ruangan kepada setiap pengguna merupakan tanggung jawab dari pegawai keamanan. Setiap pengguna yang datang ke pegawai keamanan untuk meminta akses ruangan harus bisa menunjukkan surat pengajuan akses ruangan baik dalam bentuk file ataupun *print out* serta menunjukkan kartu identitas pengguna untuk dilakukan verifikasi.

Mekanisme pemberian akses ruangan dapat dilakukan dengan dua cara yaitu secara manual dan otomatis. Jika dilakukan secara manual, pegawai keamanan harus memasukkan nomor induk pengguna, aksi yaitu menambah atau menghapus akses ruangan, serta akses ruangan yang diberikan seperti yang ditunjukkan pada Gambar 4.11.

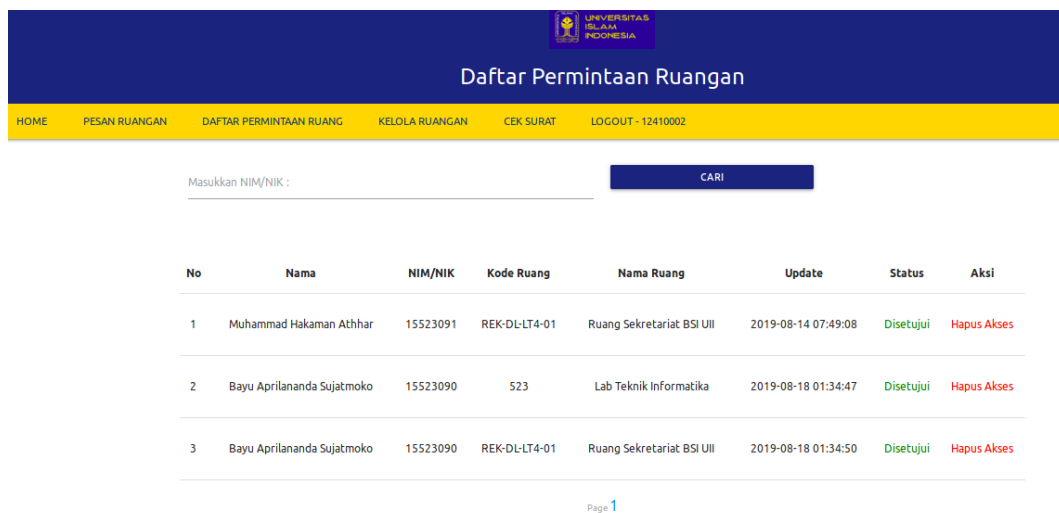


Gambar 4.11 Form Tambah/Hapus Akses Ruang Manual

Form akses ruangan manual dibuat sebagai langkah untukantisipasi apabila terjadi kerusakan/kehilangan data pada basis data MySQL yang menyimpan data setiap permintaan akses ruangan yang dibuat oleh pengguna. Sebelum akses ruangan diberikan, sistem akan mengecek apakah pengguna tersebut telah membuat daftar permintaan ruangan yang diminta sesuai dengan akses ruangan yang akan diberikan. Jika permintaan tersebut ada, maka sistem akan memberikan akses, tetapi jika permintaan tersebut tidak ada maka sistem akan menolak pemberian akses tersebut. Permasalahan yang akan timbul adalah ketika basis data MySQL rusak/terjadi kehilangan data, pegawai keamanan tidak dapat menghapus akses ruangan yang telah diberikan secara otomatis melalui halaman “Daftar Permintaan Akses Ruang” karena daftar permintaan akses ruangan telah hilang dari halaman tersebut. Untuk tujuan itulah form manual tambah/hapus akses ruangan ini dibuat.

Selain itu, mekanisme ini merupakan salah satu langkah untuk melakukan verifikasi pengguna bahwa pengguna tersebut merupakan pengguna yang valid. Selama basis data MySQL dalam keadaan baik, penulis menyarankan pegawai keamanan untuk memberikan/menghapus akses ruangan secara otomatis pada halaman “Daftar Permintaan Ruang” dengan melakukan pencarian pengguna

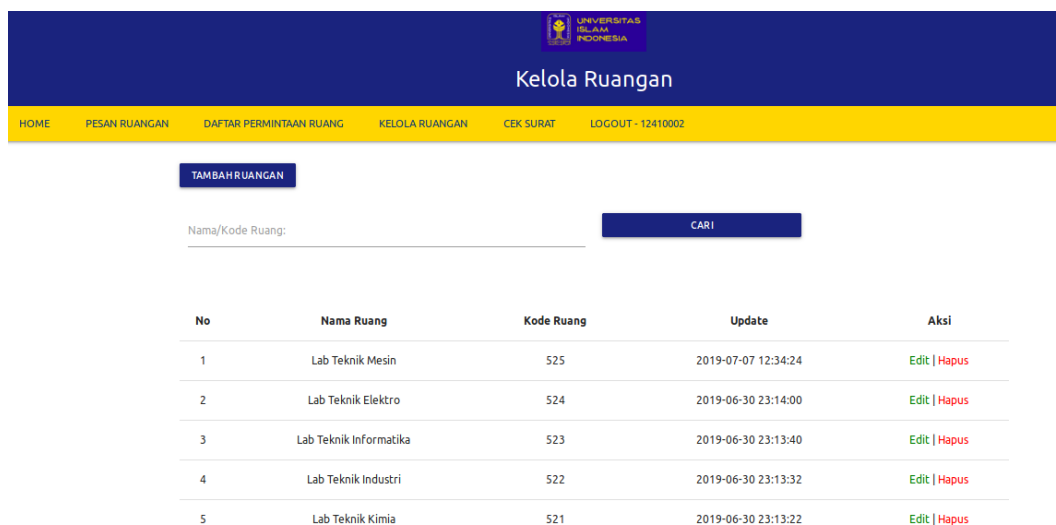
terlebih dahulu dengan alasan efisiensi waktu. Pegawai akademik juga dapat menolak permintaan akses ruangan dari pengguna yang belum disetujui seperti yang digambarkan pada Gambar 4.12.



No	Nama	NIM/NIK	Kode Ruang	Nama Ruang	Update	Status	Aksi
1	Muhammad Hakaman Athhar	15523091	REK-DL-LT4-01	Ruang Sekretariat BSI UII	2019-08-14 07:49:08	Disetujui	Hapus Akses
2	Bayu Aprilananda Sujatmoko	15523090	523	Lab Teknik Informatika	2019-08-18 01:34:47	Disetujui	Hapus Akses
3	Bayu Aprilananda Sujatmoko	15523090	REK-DL-LT4-01	Ruang Sekretariat BSI UII	2019-08-18 01:34:50	Disetujui	Hapus Akses

Gambar 4.12 Daftar Permintaan Akses Ruangan

Selain itu pegawai akademik juga dapat melakukan pengelolaan terhadap data ruangan yang meliputi nama ruang dan kode ruang yang digunakan sebagai salah satu parameter untuk proses validasi pengguna saat melakukan otentikasi ke sebuah ruangan melalui RFID reader. Pegawai akademik dapat menambah, menghapus, dan melakukan perubahan data ruangan pada halaman “Kelola Ruangan” seperti yang ditunjukkan pada Gambar 4.13.



No	Nama Ruang	Kode Ruang	Update	Aksi
1	Lab Teknik Mesin	525	2019-07-07 12:34:24	<a href="#">Edit</a>   <a href="#">Hapus</a>
2	Lab Teknik Elektro	524	2019-06-30 23:14:00	<a href="#">Edit</a>   <a href="#">Hapus</a>
3	Lab Teknik Informatika	523	2019-06-30 23:13:40	<a href="#">Edit</a>   <a href="#">Hapus</a>
4	Lab Teknik Industri	522	2019-06-30 23:13:32	<a href="#">Edit</a>   <a href="#">Hapus</a>
5	Lab Teknik Kimia	521	2019-06-30 23:13:22	<a href="#">Edit</a>   <a href="#">Hapus</a>

Gambar 4.13 Halaman Kelola Data Ruangan

Pegawai keamanan dapat mengecek surat pengajuan akses ruangan secara online dengan mengakses halaman “Cek Surat” lalu memasukkan nomor induk pengguna dan tanggal pengajuan surat tersebut melalui sebuah form seperti yang ditunjukkan pada Gambar 4.14. Hal ini dilakukan sebagai salah satu cara untuk melakukan validasi pengguna. Surat yang ditampilkan sama seperti saat pengguna membuat/mencetak surat pengajuan akses ruangan ketika menambah daftar permintaan akses ruangan.



Gambar 4.14 Halaman Cek Surat Pengajuan Akses Ruangan

#### 4.1.7 Standarisasi Penamaan Kode Ruang

Pemberian kode ruang dilakukan pada setiap RFID reader dengan melakukan konfigurasi menggunakan *smartcard* pada atribut Terminal ID. Kode ruang harus memiliki kode yang unik dan berbeda antara ruang yang satu dengan ruang yang lainnya. Standarisasi penamaan kode ruang dilakukan untuk mempermudah melakukan pengelolaan atau menelusuri setiap RFID Reader yang dipasang disetiap pintu masuk ruangan. Berikut akan disajikan sebuah contoh format penamaan salah satu kode ruang yaitu ruang sekretariat BSI UII:

REK-DL-LT4-01
---------------

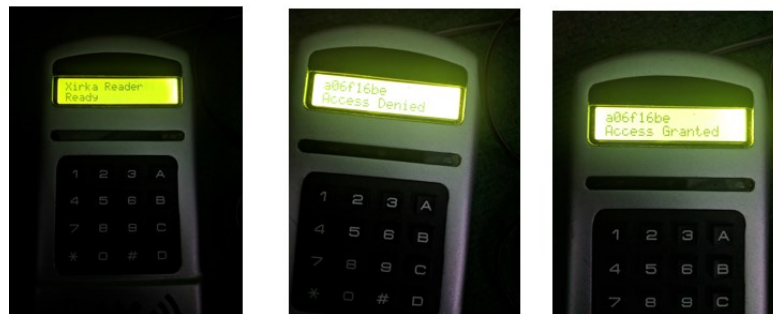
Format penamaan kode ruang di UII diikuti oleh kode nama gedung/fakultas, kode alat, lantai gedung dan nomor ruangan. Kode REK pada kode tersebut menggambarkan gedung rektorat. Kode DL menggambarkan DoorLock yang merupakan RFID Reader dan alat kunci ruangan itu sendiri. Kode LT4 berarti ruangan sekretariat BSI berada di lantai 4 dan 01 berarti ruangan sekretariat BSI bernomor ruang satu. Format inilah nantinya yang akan digunakan untuk memberi penamaan setiap kode ruang di UII. Misalnya, kita ingin memberi kode ruang dosen FTI UII yang berada di lantai 3 dengan nomor satu, maka format penamaannya adalah FTI-DL-LT3-01. Ide pemberian format penamaan kode ruang ini bersumber dari standarisasi penamaan *access point* (AP) yang telah diterapkan di UII hanya saja kode AP yang menggambarkan *access point* di UII diganti dengan DL yang menggambarkan RFID Reader dan alat kunci ruangan.

#### 4.1.8 Otentikasi Pengguna Melalui RFID Reader

Pada bagian ini akan ditunjukkan mekanisme yang terjadi di dalam server saat melakukan pengecekan pengguna melalui RFID reader ketika akan mengakses sebuah ruangan. RFID reader akan mengirimkan dua parameter data yaitu *uid card* dan kombinasi *uid card* dengan nomor ruangan (data unik) yang tidak lain adalah terminal ID dari RFID reader itu sendiri. Mekanisme pengecekan di dalam server dilakukan melalui terminal linux dengan menjalankan sebuah file “client.py” yang

berbasis python berisi kode HTTP Server untuk menerima data dari reader dan dilakukan pengecekan ke LDAP server (Microsoft Active Directory UII).

Terminal linux akan mencetak keluaran dari setiap parameter yang berhasil di cek dimana jika salah satu parameter yang dicek bernilai nol, maka pengguna tersebut tidak valid seperti yang digambarkan pada Gambar 4.15.



Gambar 4.15 Otentikasi melalui RFID Reader, Reader dalam Keadaan Ready, Status Pengguna Invalid, dan Status Pengguna Valid (dari kiri ke kanan)

#### 4.1.9 Pengamanan Info UID Tag-RFID

Setelah penulis melakukan beberapa percobaan dengan RFID Reader dari vendor Xirka dan USB RFID Reader, ternyata memiliki beberapa perbedaan terkait mekanisme saat membaca *uid* Tag dari kartu pengguna. RFID Reader dari vendor xirka menghasilkan keluaran kode *uid* dari tag kartu pengguna berupa bilangan *hexadecimal* 8 digit yang ditampilkan pada layar LCD. Sebagai bahan percobaan, saya menggunakan satu kartu pegawai dan satu kartu mahasiswa untuk mengecek *uid* tag dari masing-masing kartu. Berikut adalah kode *uid* tag dalam format *hexadecimal* yang dibaca oleh RFID Reader Xirka :



UID Tag Kartu Pegawai dalam format hexadecimal (RFID Reader Xirka):

a06f16be

UID Tag Kartu Mahasiswa dalam format hexadecimal (RFID Reader Xirka):

c06aa011

Setelah saya mengetahui format *uid* tag yang dibaca oleh RFID Reader Xirka dalam format *hexadecimal*, maka saya pun mencoba melakukan tap kartu pegawai dan kartu mahasiswa ke USB RFID Reader dan menampilkan kode *uid* tag dari kartu pada file .txt. Setelah kode *uid* kartu berhasil ditampilkan ternyata format *uid* tag yang dibaca oleh USB RFID Reader adalah bilangan *decimal* 10 digit. Hal ini tentunya terjadi perbedaan kode yang dikirimkan nantinya jika kode *uid* dari tag USB RFID Reader tidak dilakukan konversi ke dalam format *hexadecimal*. Berikut adalah kode *uid* tag dalam format *decimal* yang dihasilkan dari USB RFID Reader:

UID Tag Kartu Pegawai dalam format decimal (USB RFID Reader):

3189141408

UID Tag Kartu Mahasiswa dalam format decimal (USB RFID Reader):

0295725760

Setelah saya mengetahui *uid* tag dalam bilangan *decimal* yang dihasilkan dari USB RFID Reader, saya mencoba melakukan konversi bilangan *decimal* tersebut kedalam bentuk bilangan *hexadecimal* dan didapat hasil sebagai berikut:

UID Tag Kartu Pegawai dalam format decimal (USB RFID Reader):

be166fa0

UID Tag Kartu Mahasiswa dalam format decimal (USB RFID Reader):

11a06ac0
----------

Setelah dilakukan konversi dari bilangan *decimal* ke *hexadecimal*, dapat kita lihat bahwa kombinasi string dari bilangan *hexadecimal* RFID Reader Xirka dan USB RFID Reader tidak memiliki perbedaan, hanya letak posisi dari setiap karakter saja yang membedakannya. Perbedaan posisi karakter bilangan *hexadecimal* akan ditampilkan pada Tabel 4.1 berikut:

Tabel 4.1 Tabel Perbandingan *uid* tag *hexadecimal* antara RFID Reader Xirka dengan USB RFID Reader

	Kartu Pegawai	Kartu Mahasiswa
RFID Reader Xirka	a06f16be	c06aa011
USB RFID Reader	be166fa0	11a06ac0

Dari tabel diatas dapat kita lihat bahwa terjadi mekanisme enkripsi yang dilakukan oleh RFID Reader Xirka untuk mengamankan *uid* tag dari kartu pengguna dengan mengacak posisi karakter bilangan *hexadecimal* nya. Agar data yang dikirimkan USB RFID Reader dengan RFID Reader Xirka sama, maka kita perlu mempelajari pola posisi pengacakan dari kedua kartu tersebut. Hal ini dilakukan agar tidak terjadi perbedaan kode *uid* yang dikirimkan RFID Reader Xirka saat melakukan otentikasi dengan USB RFID Reader saat melakukan asosiasi kartu ke basis data. Jika data yang dikirimkan berbeda, maka proses otentikasi sudah pasti gagal.

Oleh karena itu diperlukan sebuah fungsi atau mekanisme untuk menyamakan kode *uid* tag RFID Reader Xirka dan USB RFID Reader yang dikirimkan ke basis data. Berikut adalah pola posisi karakter yang penulis temukan dengan melakukan perbandingan data *uid* tag dari RFID Reader Xirka dengan USB RFID Reader disajikan pada Tabel 4.2 dan Tabel 4.3 berikut:

Tabel 4.2 Tabel Pencocokan Pola Posisi Karakter UID Tag (Hexadecimal) Kartu Pegawai Pada USB RFID Reader dengan RFID Reader Xirka

Index (i)	0	1	2	3	4	5	6	7
USB RFID Reader	b	e	1	6	6	f	a	0
Pola posisi (i)	6	7	3/4	5	2	3/4	0	1
RFID Reader Xirka	a	0	6	f	1	6	b	e

Tabel 4.3 Tabel Pencocokan Pola Posisi Karakter UID Tag (Hexadecimal) Kartu Mahasiswa Pada USB RFID Reader dengan RFID Reader Xirka

Index (i)	0	1	2	3	4	5	6	7
USB RFID Reader	1	1	a	0	6	a	c	0
Pola posisi (i)	6	7	4	5	2	3	0	1
RFID Reader Xirka	c	0	6	a	a	0	1	1

Dari kedua tabel diatas, kita telah menemukan pola yang sesuai agar *uid* tag yang dibaca oleh USB RFID Reader sama atau sesuai dengan *uid* tag yang dibaca oleh RFID Reader Xirka dengan membandingkan *uid* tag dari dua kartu yang berbeda. Pola posisi pengacakan karakter *uid* tag yang didapat dari kedua kartu adalah sama dilihat dari pola posisi (i) perubahan index karakter *uid* tag dari kedua kartu, sehingga penulis dapat menyesuaikan agar data yang dikirimkan dari USB RFID Reader dengan RFID Reader Xirka ke dalam basis data adalah sama.

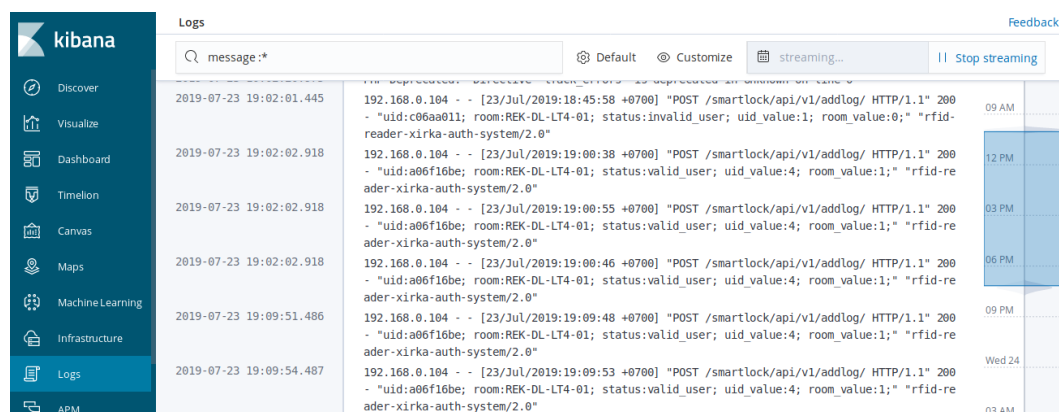
#### 4.1.10 Pemantauan Aktivitas Log RFID Reader

Saat pengguna melakukan tap kartu ke RFID reader, reader akan melakukan pencatatan log dari setiap pengguna yang mencoba melakukan otentikasi untuk mendapatkan akses ruangan. RFID reader akan mencatat pengguna yang valid dan invalid ke dalam sebuah log file berekstensi .log yang nantinya akan di parsing ke dalam format yang dapat dibaca oleh Elasticsearch, Logstash dan Kibana.

*Kibana* adalah sebuah antarmuka yang digunakan untuk melakukan visualisasi dari *log*. *Kibana* memerlukan *Elasticsearch* dan *Logstash*. *Logstash* bertugas untuk mengambil log dari hasil logging yang dilakukan oleh protokol LDAP atau web server Apache sedangkan *Elasticsearch* bertugas untuk melakukan pengumpulan data dari *log* yang selanjutnya data *log* tersebut digunakan *Kibana* untuk di visualisasikan. File log yang dihasilkan dari RFID reader disesuaikan dengan format log apache untuk memudahkan peneliti melakukan parsing log agar dapat dibaca oleh kibana. Contoh format log apache dalam satu baris adalah sebagai berikut:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif
HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08
[en] (Win98; I ;Nav) "
```

Untuk lebih jelasnya format log apache (message) yang berhasil di tampilkan kedalam logs kibana akan digambarkan pada Gambar 4.16.

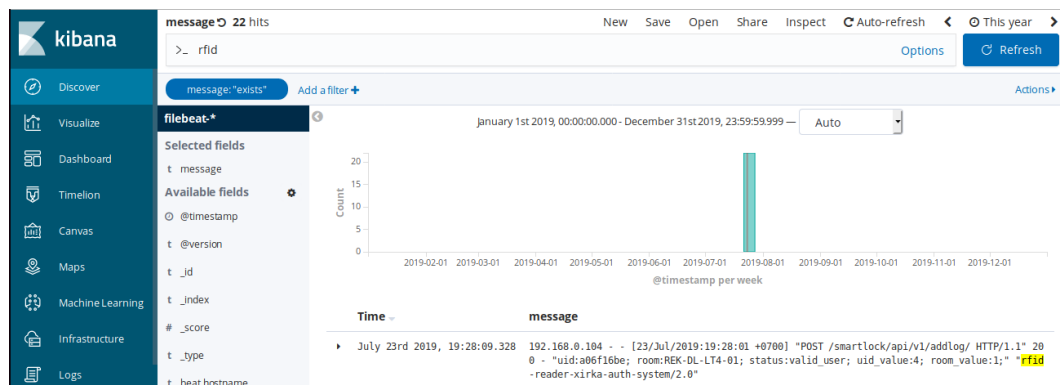


Gambar 4.16 Logs Message RFID Reader di Kibana

Pada gambar diatas format log RFID reader sudah disesuaikan dengan format log apache agar mudah untuk dibaca oleh *tools* ELK, format log RFID reader dalam satu baris adalah sebagai berikut:

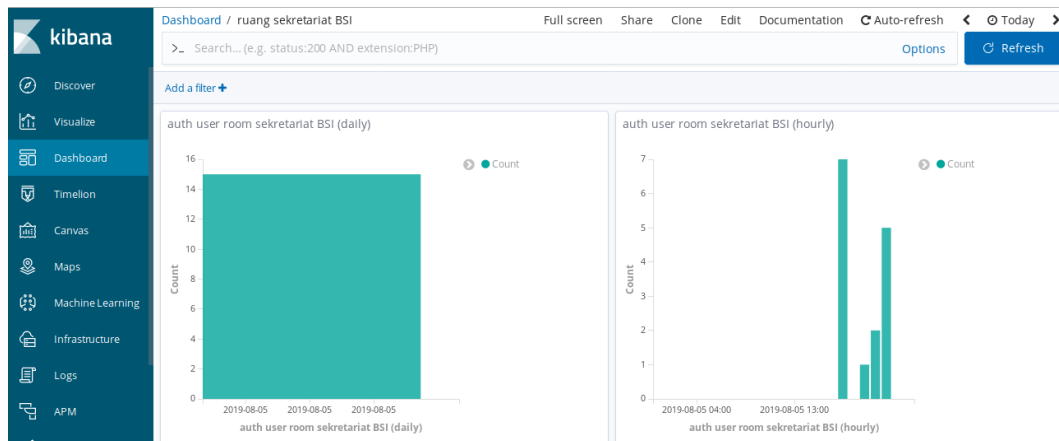
```
192.168.0.104 - - [23/Jul/2019:19:00:55 +0700] "POST
/smartlock/api/v1/addlog/ HTTP/1.1" 200 - "uid:a06f16be;
room:REK-DL-LT4-01; status:valid_user; uid_value:4;
room_value:1;" "rfid-reader-xirka-auth-system/2.0"
```

Sebagai tanda bahwa log dari RFID reader juga telah berhasil di tampilkan ke dalam *tools* Kibana, log tersebut juga akan muncul pada tampilan “Discover” Kibana yang menampilkan seluruh log dari sistem. Untuk menampilkan data dari RFID reader sesuai dengan yang kita inginkan, maka dilakukan filter message dengan keyword rfid maka akan tampil seperti pada Gambar 4.17.

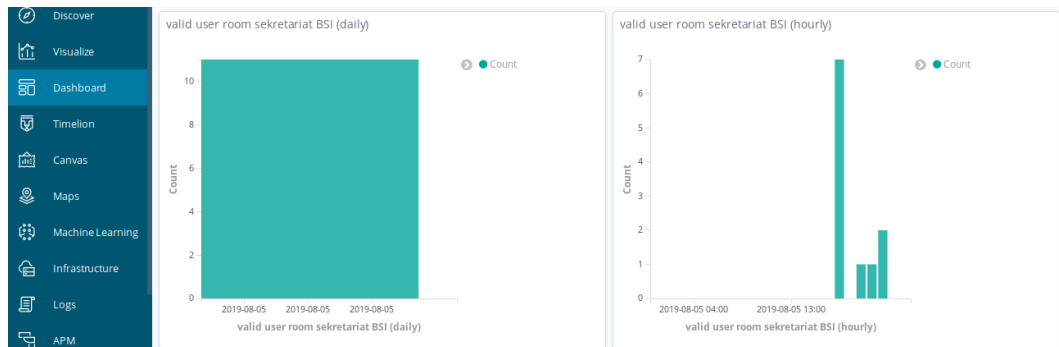


Gambar 4.17 Log RFID Reader pada Bagian Discover Kibana

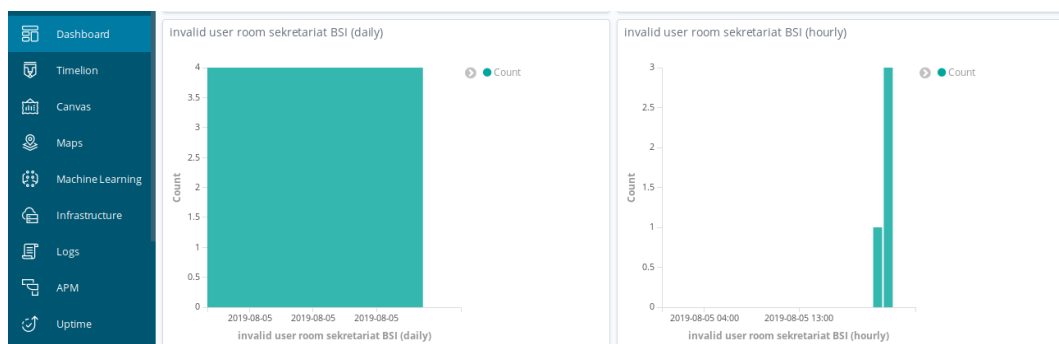
Visualisasi log dari RFID reader ditampilkan dalam bentuk *grafik* untuk menampilkan jumlah pengguna yang melakukan otentikasi, pengguna valid atau pengguna yang tidak valid saat akan melakukan otentikasi ke sebuah ruangan tertentu. Grafik ditampilkan dalam bentuk *time series* yang pada penelitian ini ditampilkan berdasarkan jam dan hari untuk mengamati *trend* saat menggunakan ruangan tertentu. Berikut adalah tampilan visualisasi dari log RFID reader yang digambarkan pada Gambar 4.18, Gambar 4.19, dan Gambar 4.20.



Gambar 4.18 Visualisasi Jumlah Pengguna Otentikasi ke Sebuah Ruangan



Gambar 4.19 Visualisasi Jumlah Pengguna Valid ke Sebuah Ruangan



Gambar 4.20 Visualisasi Jumlah Pengguna Tidak Valid ke Sebuah Ruangan

## 4.2 Hasil Pengujian Sistem

Pada penelitian ini penulis menggunakan teknik pengujian aplikasi *Black Box*. *Black Box* testing dilakukan untuk mengetahui apakah aplikasi yang telah dibangun sebelumnya dapat berjalan sesuai dengan kebutuhan fungsional pengguna. *Black Box* biasa digunakan untuk menemukan beberapa kesalahan dalam aplikasi yang telah dibangun seperti fungsi yang tidak sesuai, kesalahan *interface*, batasan dari suatu data dsb. Pengujian *Black Box* terdiri dari enam tipe yaitu *Equivalence Partitioning*, *Sample Testing*, *Limit Testing*, *Robustness Testing*, *Behaviour Testing*, dan *Requirement Testing*.

Penulis memilih tipe *Equivalence Partitioning* sebagai metode pengujian *Black Box* pada aplikasi ini. *Equivalence Partitioning* akan membagi domain masukan ke dalam beberapa kelas yang dijadikan sebagai kasus (Ikhlashi, 2016). Kelas yang telah dibentuk akan disajikan sebagai kondisi masukan di dalam kasus uji dimana kelas tersebut terdiri dari nilai yang *valid* dan tidak *valid*. Kondisi masukan (input) bisa beragam contohnya seperti text, angka, rentang nilai, suatu himpunan, atau boolean. Hal inilah yang menjadi dasar penulis memilih metode ini sebagai langkah pengujian aplikasi akses kontrol ruang ini karena dirasa lebih tepat dan sesuai dengan sistem yang akan diuji.

Hasil pengujian dilakukan di lingkungan BSI UII bersama-sama dengan tim dari DevOps4 yang terdiri dari 4 orang. Hasil pengujian sistem untuk semua fitur mendapatkan hasil yang baik karena sebagian besar dari fitur yang diuji sesuai dengan kebutuhan pengguna dan berhasil. Hal ini menunjukkan bahwa sistem dapat berjalan dengan lancar secara keseluruhan. Parameter hasil pengujian dari sistem aplikasi akses kontrol ruang akan ditunjukkan pada Tabel 4.4 berikut:

Tabel 4.4 Hasil Pengujian (Equivalence Partitioning) pada Sistem Akses Kontrol Ruang

No	Pengujian	Detail	Output	Hasil Uji	
				Berhasil	Gagal
1.	Fungsi halaman login	Login sebagai pengguna umum (civitas akademik)	Menampilkan halaman <i>home</i> pengguna umum yaitu form pengajuan akses ruangan	1	0
		Login sebagai pegawai akademik	Menampilkan halaman <i>home</i> pegawai akademik yaitu form asosiasi kartu pengguna	1	0
		Login sebagai pegawai keamanan	Menampilkan halaman <i>home</i> pegawai keamanan yaitu form tambah/hapus akses ruangan manual	1	0
		Proses pengecekan pengguna yang tidak valid	Menampilkan pesan “Kesalahan userpass/group. Asosiasikan kartu terlebih dahulu”	1	0
		Proses pengecekan field username masih kosong	Menampilkan pesan “username belum diisi”	1	0
		Proses pengecekan field password masih kosong	Menampilkan pesan “password belum diisi”	1	0
2.	Fungsi sistem aplikasi pesan ruang (pengguna umum)	Proses menambah permintaan akses ruangan (halaman <i>home</i> pengguna umum)	Menampilkan pesan “data berhasil ditambahkan” dan menampilkan daftar permintaan akses ruangan pada halaman berikutnya	1	0



		Proses pengecekan field nama; nomor induk; ruangan; pada form tambah permintaan akses ruang jika kosong	Menampilkan pesan “nama belum diisi”; “nomor induk belum diisi”; “ruangan belum diisi”;	1	0
		Melihat daftar permintaan akses ruangan	Menampilkan informasi daftar permintaan akses ruangan meliputi nama, nomor induk, kode ruang, nama ruang, update, dan status (disetujui/tidak)	1	0
		Proses mencetak surat pengajuan akses ruangan	Menampilkan bentuk <i>print out</i> surat pengajuan akses ruangan	1	0
		Proses pengecekan belum membuat permintaan akses ruangan saat mencetak surat pengajuan pada hari yang sama	Menampilkan pesan “Belum membuat permintaan akses ruangan pada hari ini”	1	0
		Melihat daftar akses ruangan	Menampilkan informasi akses ruangan yang diberikan meliputi id card, username, nama, email, dan akses ruangan	1	0
3.	Fungsi sistem aplikasi asosiasi kartu	Proses melakukan cek saat melakukan	Menampilkan pesan “Pengguna tidak ditemukan”	1	0

	pengguna ke basis data LDAP	asosiasi kartu jika data pengguna tidak ditemukan			
	(pegawai akademik)	Proses mengambil data <i>uid card</i> dari RFID reader ke form aplikasi asosiasi kartu pengguna dengan melakukan tap kartu ke reader secara otomatis menggunakan USB RFID Reader	Menampilkan <i>uid card</i> pada form aplikasi asosiasi kartu pengguna	1	0
		Proses mengecek field <i>uid card</i> ; nomor induk; pada form asosiasi kartu pengguna jika kosong.	Menampilkan pesan “ID card belum diisi”; “nomor induk belum diisi”	1	0
		Proses melakukan asosiasi kartu pengguna ke basis data LDAP	Menampilkan pesan “Entri berhasil dimodifikasi. ID card berhasil diubah/ditambahkan dan user berhasil dimasukkan kedalam group xirka” pada halaman berikutnya dan menampilkan informasi pengguna seperti ID card, username, nama, email	1	0

4.	Fungsi sistem aplikasi tambah/hapus akses ruangan pengguna (pegawai keamanan)	Proses mengecek field nomor induk; aksi (tambah/hapus akses ruang); akses ruangan; pada form tambah/hapus akses ruangan pengguna jika kosong.	Menampilkan pesan “nomor induk belum diisi”; “kesalahan input data/opsi belum dipilih”; “ruangan belum diisi”	1	0
		Proses memberikan akses ruangan manual kepada pengguna melalui form tambah/hapus akses ruangan manual	Menampilkan pesan “Entri berhasil dimodifikasi. Akses ruangan yang baru telah ditambahkan” jika berhasil. Menampilkan pesan “Entri berhasil dimodifikasi. Pengguna belum melakukan asosiasi kartu atau belum mengajukan permintaan akses ruangan” dan “Akses ruangan yang ingin ditambahkan sudah ada” jika gagal.	1	0
		Proses memberikan akses ruangan secara otomatis kepada pengguna dengan menekan tombol “beri akses” melalui halaman daftar permintaan akses ruangan	Lalu menampilkan informasi pengguna seperti ID card, username, nama, email, akses ruangan	1	0

	Proses menghapus akses ruangan manual kepada pengguna melalui form tambah/hapus akses ruangan manual	Menampilkan pesan “Entri berhasil dimodifikasi. Salah satu akses ruangan telah dihapus” jika berhasil. Menampilkan pesan “Entri berhasil dimodifikasi. Akses ruangan yang ingin dihapus tidak ada” jika gagal. Lalu menampilkan informasi	1	0
	Proses menghapus akses ruangan secara otomatis kepada pengguna dengan menekan tombol “hapus akses” melalui halaman daftar permintaan akses ruangan	pengguna seperti ID card, username, nama, email, akses ruangan	1	0
	Proses menolak permintaan akses ruangan pada halaman daftar permintaan akses ruangan	Menghapus akses ruangan yang diminta oleh pengguna	1	0
	Proses mencari data pengguna pada halaman tambah/hapus akses ruangan manual	Menampilkan pesan “user ditemukan” lalu menampilkan informasi pengguna seperti ID card, username, nama, email, akses ruangan jika berhasil.	1	0

			Menampilkan pesan “user tidak ditemukan” jika gagal		
		Proses mencari daftar permintaan akses ruangan yang diminta oleh pengguna berdasarkan nomor induk pada halaman daftar permintaan akses ruangan	Menampilkan daftar permintaan akses ruangan yang diminta oleh pengguna berdasarkan nomor induk	1	0
		Proses mengecek apakah pengguna belum melakukan asosiasi kartu atau membuat permintaan akses ruangan oleh sistem saat pegawai akademik ingin memberikan akses ruangan	Menampilkan pesan “Pengguna belum melakukan asosiasi kartu atau permintaan akses ruangan belum dibuat”	1	0
		Proses menambah daftar ruangan	Menampilkan pesan “data berhasil ditambahkan” dan menambah daftar ruangan	1	0
		Proses mengecek field kode ruang; nama ruang; pada form tambah	Menampilkan pesan “kode ruang belum diisi”; “nama ruang belum diisi”	1	0

		ruangan pengguna jika kosong.			
		Proses mengecek field kode ruang; nama ruang; pada form edit ruangan pengguna jika kosong.		1	0
		Proses melakukan edit data ruangan pada halaman form edit data ruang	Menampilkan pesan “data berhasil diedit” dan data ruang berhasil diubah sesuai ketentuan pengguna	1	0
		Proses mencari data ruangan berdasarkan kode ruang atau nama ruang	Menampilkan data ruangan berdasarkan kode ruang atau nama ruang yang dicari	1	0
		Proses menghapus data ruang	Menampilkan pesan “data berhasil dihapus” dan data ruangan yang dihapus telah terhapus	1	0
		Proses cek <i>print out</i> surat pengajuan akses ruangan dengan mengisi nomor induk dan tanggal pembuatan surat pada form	Menampilkan surat pengajuan akses ruangan dalam bentuk <i>print out</i> berdasarkan nomor induk dan tanggal pembuatan surat yang sesuai kriteria pengguna	1	0

		Proses mengecek field nomor induk; tanggal; pada form cek surat pengajuan akses ruangan jika kosong	Menampilkan pesan “nomor induk belum diisi”; “tanggal belum diisi”	1	0
5.	Fungsi otentikasi RFID reader xirka	Proses RFID reader berhasil terhubung ke jaringan Wifi untuk melakukan komunikasi dengan server	Menampilkan pesan “Update RTC Success” dan “Xirka Reader Ready” reader terhubung ke jaringan Wifi dan berkomunikasi dengan server	1	0
		Proses RFID reader berhasil melakukan validasi pengguna yang valid saat melakukan otentikasi	Menampilkan pesan “Access Granted” dan kunci akan terbuka	1	0
		Proses RFID reader berhasil melakukan validasi pengguna yang tidak valid saat melakukan otentikasi	Menampilkan pesan “Access Denied” dan kunci akan tetap tertutup	1	0
		Proses RFID reader gagal	Menampilkan pesan “invalid card” dan “Timeout”	1	0

		mevalidasi kartu dan gagal terhubung ke server			
		Proses RFID reader mencatat log pengguna yang melakukan otentikasi	Menampilkan <i>message</i> log dalam format apache pada file <code>access.log</code> ( <code>/var/log/apache2/access.log</code> )	1	0
		Proses RFID reader mencatat log pengguna yang valid saat melakukan otentikasi	Menampilkan potongan <i>message</i> log “status:valid_user”	1	0
		Proses RFID reader mencatat log pengguna yang tidak valid saat melakukan otentikasi	Menampilkan potongan <i>message</i> log “status:invalid_user”	1	0
6.	Fungsi menampilkan Log RFID reader menggunakan Elasticsearch, Logstash, Kibana (ELK)	Proses membaca log RFID reader dari file <code>apache.log</code> sesuai format log web server apache	Menampilkan <i>message</i> log RFID reader pada halaman <code>discover kibana</code>	1	0



		Proses melakukan visualisasi data pengguna yang melakukan autentikasi melalui RFID reader baik yang valid, yang tidak valid, dan gabungan keduanya (yang melakukan autentikasi)	Menampilkan data pengguna yang valid dan tidak valid saat melakukan autentikasi ke RFID reader dalam bentuk grafik dan menghitung jumlah pengguna yang valid, tidak valid, dan gabungan keduanya (yang melakukan autentikasi)	1	0
7.	Fungsi Blokir Akses Ruang Pengguna	Proses melakukan blokir akses ruangan pengguna dengan memasukkan data nomor_induk pengguna	Menampilkan pesan “Semua akses ruangan pengguna berhasil dihapus” jika akses ruangan berhasil diblokir dan menampilkan pesan “Akses ruangan pengguna tidak tersedia” jika gagal	1	0
		Proses menampilkan informasi data pengguna bahwa kartu dan akses ruangan telah diblokir	Menampilkan data pengguna dan info kartu bahwa kartu sudah tidak diasosiasikan ke basis data LDAP	1	0