BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Untuk menjawab rumusan masalah yang telah dipaparkan pada bab I, penulis menggunakan salah satu pendekatan dari metode *Software Development Life Cycle* (Dora & Dubey, 2013) yaitu metode *waterfall* untuk mengerjakan tugas akhir ini. Secara lebih spesifik, penelitian ini akan dilakukan dengan beberapa tahapan berikut.

3.1.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk menentukan cara kerja dan manfaat sistem yang akan dikembangkan nantinya. Analisis kebutuhan sistem merepresentasikan segala hal yang dibutuhkan terkait pengembangan sistem keamanan ruang menggunakan teknologi RFID di Universitas Islam Indonesia. Dengan melakukan analisis kebutuhan sistem akan memudahkan penulis untuk memberikan gambaran perancangan yang akan dilakukan. Analisis kebutuhan sistem yang dilakukan meliputi kebutuhan perangkat lunak dan perangkat keras.

a. Tahapan Analisis Kebutuhan

Hal-hal yang perlu dilakukan dalam melakukan analisis kebutuhan sistem untuk melakukan pengembangan sistem keamanan ruang di BSI UII yaitu:

Wawancara

Pada tahap ini dilakukan wawancara kepada pihak-pihak BSI UII dan pihak Xirka Silicon Techonology selaku pembuat dan pengembang RFID-reader yang terlibat dalam hal pengembangan sistem sebelumnya. Hal ini dilakukan agar peneliti dapat memahami arsitektur dari sistem yang telah berjalan sebelumnya sehingga dapat dilakukan analisis untuk pengembangan selanjutnya.

Studi Literatur

Pada tahap ini dilakukan studi literatur mengenai cara instalasi dan *set up* RADIUS, Kibana, *Active Directory*, LDAP serta mengintegrasikannya menggunakan RFID dengan mempelajari dari berbagai sumber dan dokumentasi yang ada. Studi literatur dilakukan dengan membaca jurnal dan penelitian yang sudah dilakukan.

Pengumpulan Data Pengguna

Pada tahap ini melakukan pengumpulan data pengguna melalui RFID-tag *card* yang kemudian akan dibaca oleh RFID *reader* dan diproses oleh komputer. UID dari RFID-tag akan disimpan di dalam akun LDAP *Active Directory*. Pada tahap ini perlu dilakukan kerja sama dengan vendor Xirka Silicon Technology selaku pembuat dari RFID-reader untuk mengetahui cara kerja dari RFID-reader agar dapat dikembangkan sesuai kebutuhan di BSI UII.

b. Kebutuhan Perangkat Lunak

Perangkat lunak yang dibutuhkan untuk melakukan pengembangan sistem keamanan ruang menggunakan teknologi RFID agar dapat berjalan dalam melakukan pengelolaan otentikasi dan validasi pengguna serta mendaftarkan pengguna baru di lingkungan Universitas Islam Indonesia adalah sebagai berikut:

1. *Ubuntu:* Sistem operasi Ubuntu dalam penelitian ini digunakan untuk mengembangkan aplikasi *backend* untuk pendaftaran pengguna baru (asosiasi informasi RFID-tag ke basis data) serta melakukan simulasi pembuatan sistem.
2. *LDAP:* protokol LDAP digunakan untuk mengasosiasikan *idcard* didalam RFID-tag ke dalam basis data akun pengguna *Active Directory*. Disini peneliti menggunakan phpLDAPadmin sebagai sarana untuk mengembangkan sistem secara lokal di *localhost*, namun implementasinya akan memanfaatkan Microsoft Active Directory

3. *phpLDAPadmin:* Perangkat lunak yang digunakan untuk membuat simulasi daftar akun pengguna di dalam *Active Directory* selama pengembangan sistem.
4. *Microsoft Active Directory:* Perangkat lunak *Active Directory* sebenarnya yang digunakan UII, dimana nantinya aplikasi *backend* keamanan ruang ini akan diterapkan menggunakan basis data akun pengguna *Microsoft Active Directory. Microsoft Active Directory* dan *phpLDAPadmin* sama-sama menggunakan protol LDAP.
5. *Elasticsearch, Logstash, Kibana:* Perangkat lunak yang digunakan untuk memvisualisasikan pencatatan log.

c. Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan untuk membangun sistem aplikasi *backend* keamanan ruang di UII membutuhkan 1 buah server dengan sistem operasi Linux/Ubuntu, RFID-tag (kartu pengguna/smartcard), RFID-reader digunakan untuk membaca RFID-tag kartu pengguna, *MasterCard Editor*, dan *mastercard* yang digunakan untuk konfigurasi RFID Reader. Berbagai perangkat keras yang dibutuhkan digambarkan pada Gambar 3.1 berikut :

Gambar 3.1 Kebutuhan Perangkat Keras

Dari kiri ke kanan: RFID-reader (xirka), RFID-tag (smartcard), *Mastercard Editor*, *Mastercard*

Saat ini, Universitas Islam Indonesia sudah menggunakan kartu elektronik sebagai identitas dari masing-masing pengguna yang dapat digunakan untuk berbagai macam keperluan salah satunya yaitu otentikasi pengguna. UII menggunakan RFID-tag *passive* jenis Mifare Classic dikarenakan ukurannya yang tipis, ringan, dan tidak memerlukan baterai untuk penggunaannya serta harganya yang murah. Selain itu UII juga menggunakan RFID-reader buatan salah satu vendor asal Bandung yaitu Xirka Silicon Technology sehingga dibutuhkan kerjasama terhadap vendor tersebut agar sistem ini dapat dikembangkan sesuai kebutuhan di UII. RFID Reader Xirka digunakan untuk melakukan otentikasi saat pengguna mengakses sebuah ruangan dan memberi perintah untuk membuka atau mengunci gembok pada pintu. RFID Reader Xirka memiliki layar LCD yang berfungsi untuk menampilkan informasi *uid* tag dari kartu pengguna.

USB RFID Reader digunakan untuk mengirim data *uid card* ke salah satu field di form aplikasi web. USB *RFID Reader* bersifat *plug and play* yaitu perangkat keras yang tanpa perlu dilakukan pemasangan aplikasi tambahan ketika akan digunakan. USB RFID Reader langsung siap untuk digunakan saat dihubungkan ke komputer dan dapat membaca *uid* dari tag kartu pengguna serta menampilkannya pada bagian *cursor* yang sedang aktif. USB RFID reader yang digunakan adalah USB RFID Reader dengan frekuensi 13.56 MHz yang digunakan untuk membaca tag Mifare Classic. USB RFID Reader ditunjukkan pada Gambar 3.2.

Gambar 3.2 USB RFID Reader

d. Kebutuhan Fungsional

Setelah melakukan studi literatur dan wawancara dengan pihak BSI UII terkait pengembangan sistem keamanan ruang menggunakan RFID di BSI UII, penulis memahami paling tidak terdapat enam kebutuhan fungsionalitas yang akan dikembangkan didalam sistem ini yaitu otentikasi pengguna ruangan, aplikasi asosiasi kartu dengan akun LDAP, aplikasi tambah/hapus akses pengguna ruangan, dan pencatatan serta visualisasi pencatatan aktivitas sistem atau log, aplikasi pengajuan akses ruangan, dan aplikasi blokir akses ruangan jika terjadi kehilangan kartu.

Aplikasi otentikasi pengguna ruangan memiliki fungsi untuk memberikan akses kepada pengguna saat akan menggunakan atau masuk kedalam sebuah ruang. Hal ini dilakukan dengan melakukan otentikasi terhadap pengguna bahwa pengguna tersebut benar-benar teregistrasi untuk mengakses sebuah ruangan dengan id kartu dan nomor ruangan yang sama (valid). *Stackholder* yang nantinya dapat menggunakan fitur ini yaitu semua civitas akademik di UII.

Aplikasi asosiasi kartu dengan akun LDAP memiliki fungsi untuk mendaftarkan UID kartu pengguna ke akun LDAP yang nantinya digunakan untuk keperluan otentikasi. *Stackholder* yang dapat menggunakan fitur ini nantinya yaitu pegawai akademik.

Aplikasi tambah/hapus akses pengguna ruangan memiliki fungsi untuk mendaftarkan nomor ruangan ke dalam akun LDAP yang nantinya juga akan diperlukan untuk keperluan otentikasi dengan mencocokkan UID kartu dan nomor ruangan yang akan diakses pengguna dengan yang terdaftar di akun LDAP. Hal ini bertujuan untuk mendaftarkan pengguna baru yang akan diberikan akses untuk menggunakan sebuah ruangan. *Stackholder* yang dapat menggunakan fitur ini nantinya yaitu pegawai keamanan (security).

Pencatatan dan *visualisasi aktivitas sistem (log)*. Sistem diharapkan memiliki kemampuan untuk mencatat transaksi yang terjadi selama sistem digunakan seperti menghitung jumlah pengguna yang melakukan otentikasi, baik pengguna yang valid maupun yang tidak valid.

Aplikasi Pengajuan Akses Ruangan memiliki fungsi untuk membuat daftar permintaan akses sebuah ruangan yang keluarannya adalah sebuah surat. Surat tersebut nantinya dibawa kepada petugas keamanan dengan menunjukkan kartu pegawai atau kartu mahasiswa agar petugas keamanan dapat memberikan akses ruangan kepada pengguna tersebut. Surat tersebut berfungsi sebagai bukti bahwa data pengguna benar-benar valid dan berintegritas.

Aplikasi Blokir Akses Ruangan Pengguna memiliki fungsi untuk menghapus semua akses ruangan pengguna jika terjadi kehilangan kartu. Hal ini diperlukan agar akses ruangan yang diberikan pada kartu yang hilang tidak disalahgunakan oleh pihak lain.

Kebutuhan fungsionalitas sistem keamanan ruang menggunakan RFID di BSI UII akan digambarkan pada Gambar 3.3 berikut dalam bentuk infografis:

Gambar 3.3 Infografis Kebutuhan Fungsionalitas Sistem Keamanan Ruang Menggunakan RFID di BSI UII

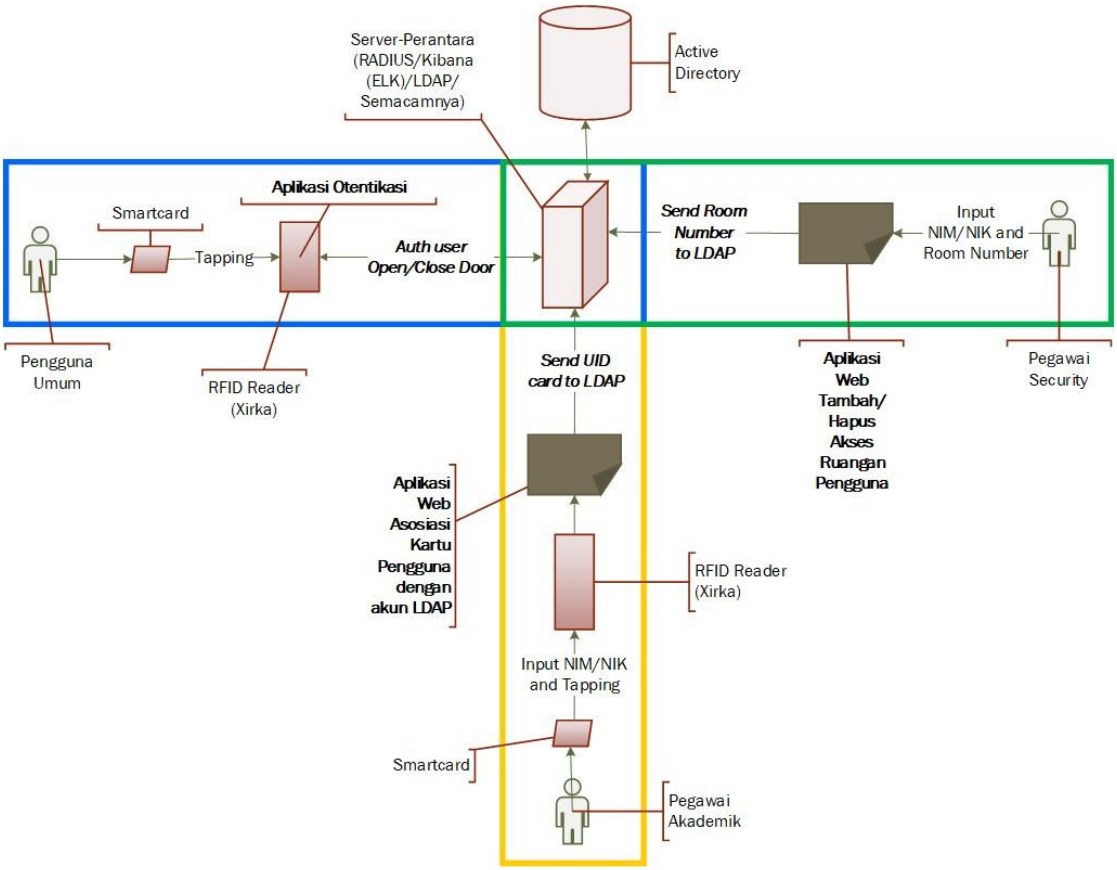
Selain kebutuhan fungsionalitas diatas, dibutuhkan satu kebutuhan sistem lagi diluar kebutuhan fungsionalitas tersebut yang berguna untuk mendukung jalannya

proses bisnis saat pengguna ingin mengajukan akses sebuah ruangan yaitu sebuah aplikasi untuk mengecek surat pengajuan akses ruangan secara digital yang dapat dilakukan oleh petugas keamanan sebagai salah satu cara untuk melakukan verifikasi permintaan akses ruangan secara *online*.

3.1.2 Perancangan

Perancangan dilakukan untuk menentukan spesifikasi perangkat keras dan perangkat lunak yang sesuai dengan kebutuhan. Kegiatan ini menentukan arsitektur sistem secara keseluruhan dan cara kerja sistem. Desain keamanan ruang menggunakan teknologi RFID paling tidak memiliki fokus kedalam empat permasalahan yang sangat fundamental yaitu audit, manajemen, kontrol akses, dan otentikasi (Rieback, Gaydadjiev, Crispo, Hofman, & Tanenbaum, 2006). Oleh karena itu untuk membangun sistem keamanan ruang yang utuh teknologi RFID tidak bisa berdiri sendiri untuk memenuhi penyelesaian dari empat permasalahan yang sangat fundamental tersebut, maka dibutuhkan elemen lain seperti basisdata, *backend* aplikasi, RFID-Reader, dan RFID-tag yang saling terintegrasi satu dengan yang lainnya menjadi suatu sistem yang utuh (Verma & Tripathi, 2010).

Berdasarkan paparan di atas, BSI UII akan mengembangkan sebuah sistem pengamanan ruang dengan menggunakan teknologi RFID. Teknologi RFID ini akan diintegrasikan dengan protokol LDAP pada *Active Directory* yang memuat seluruh informasi akun pengguna di UII. Hal ini bertujuan untuk mempermudah dalam proses otentikasi karena otentikasi pengguna saat melakukan akses sebuah ruangan akan dilakukan secara terpusat. Secara umum sistem keamanan ruang yang akan dikembangkan ini memiliki beberapa fungsi utama yaitu otentikasi, asosiasi *smartcard* dengan akun LDAP, menambah atau menghapus akses ruangan pengguna, serta audit berupa pencatatan aktivitas (log) menggunakan kibana. Untuk lebih jelasnya, rancangan arsitektur sistem keamanan ruang menggunakan RFID akan digambarkan pada Gambar 3.4 berikut:



Gambar 3.4 Rancangan Arsitektur Sistem Keamanan Ruang Menggunakan RFID di BSI UII

Berdasarkan rancangan sistem tersebut terdapat tiga *stackholder* yang nantinya akan berperan dalam menggunakan sistem tersebut yaitu pengguna secara umum, pegawai akademik, dan pegawai security. Pengguna secara umum merupakan orang yang nantinya akan melakukan akses sebuah ruangan dengan melakukan *tapping smartcard* ke RFID-reader untuk melakukan otentikasi yang berkaitan dengan seluruh civitas akademik yang berada di UII. Pegawai akademik memiliki peran untuk melakukan asosiasi kartu identitas pengguna (smartcard) dengan akun LDAP *Active Directory* menggunakan RFID-reader agar seluruh pengguna yang akan mengakses ruangan nantinya benar-benar telah teregistrasi. Asosiasi kartu ini dapat dilakukan oleh pegawai akademik terhadap pengguna yang benar-benar pengguna baru karena belum pernah melakukan asosiasi kartu ke akun LDAP *Active Directory* dan pengguna lama namun mengalami kehilangan kartu

sehingga harus dibuat kartu baru dan dilakukan asosiasi ulang kartu ke akun LDAP *Active Directory* menggunakan UID-card yang baru. Pegawai keamanan (security) memiliki peran untuk memberikan, menghapus dan melihat akses ruangan yang telah diberikan kepada pengguna ruangan. Hal ini bertujuan agar akses terhadap sebuah ruangan benar-benar diberikan kepada pengguna yang teregistrasi dengan nomor ruangan tersebut.

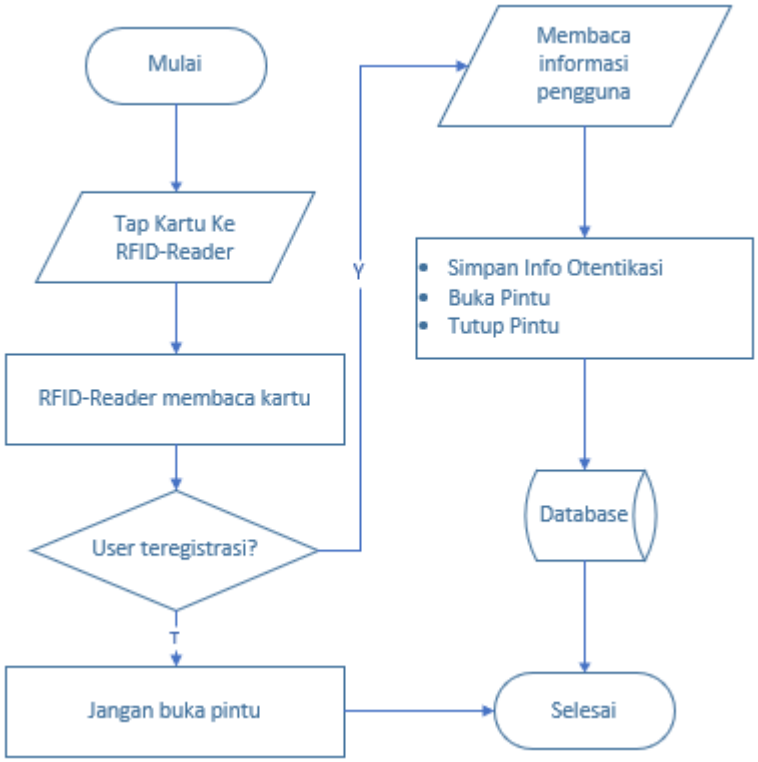
Sebuah aplikasi kecil nantinya akan dirancang untuk memenuhi kebutuhan peran dari ketiga *stackholder* tersebut adalah aplikasi otentikasi pengguna ruangan, aplikasi asosiasi kartu dengan akun LDAP, dan aplikasi untuk menambahkan dan menghapus akses ruangan pengguna.

3.1.2.1 Rancangan Aplikasi Otentikasi Pengguna Ruangan

Pada sistem sebelumnya, otentikasi pengguna hanya dilakukan dengan melakukan pengecekan apakah username yang terdapat pada *smartcard* pengguna teregistrasi dengan akun LDAP sehingga tidak ada validasi pengguna disana. Disisi lain, hal ini tentunya tidak efisien karena username yang terdapat pada kartu pengguna bukanlah identitas asli dari *smartcard* sehingga harus merubah isi kartu tersebut. Hal ini akan sangat menyita waktu ketika terdapat ribuan pengguna.

Pada rancangan aplikasi otentikasi yang baru ini, nantinya UID-card dari *smartcard* yang dimiliki oleh setiap pengguna akan diasosiasikan dengan akun LDAP sehingga UID-card tersebut tersimpan didalam basisdata. Oleh karena itu nantinya akan ditambahkan dua buah atribut pada akun LDAP yaitu UID-card dan *roomNumber* yang akan digunakan untuk otentikasi dan validasi pengguna.

Ketika akan mengakses sebuah ruangan pengguna melakukan *tapping* kartu ke RFID-reader. Lalu RFID-reader membaca kartu dan mengirim data ke komputer untuk diproses, apabila teregistrasi maka pintu akan terbuka. Diagram alur otentikasi pengguna saat mengakses ruangan digambarkan pada berikut:



Gambar 3.5 Diagram Alur Otentikasi Pengguna saat Akses Ruangan

3.1.2.2 Rancangan Aplikasi Permintaan Akses Ruangan

Untuk mendukung jalannya proses bisnis, maka dirancang sebuah aplikasi yang akan digunakan oleh pengguna untuk membuat daftar permintaan akses ke sebuah ruangan yang keluarannya dalam bentuk surat. Surat tersebut nantinya dibawa oleh pengguna tersebut kepada petugas keamanan dengan menunjukkan kartu pegawai atau kartu mahasiswa agar petugas keamanan tersebut dapat melakukan validasi bahwa pengguna tersebut adalah civitas akademik di UII. Setelah melakukan validasi petugas keamanan tersebut dapat memberikan akses ke sebuah ruangan yang diminta oleh pengguna tersebut. Aplikasi ini nantinya dapat diakses oleh tiga *stackholder* yaitu pengguna umum, pegawai akademik, dan petugas keamanan. Untuk lebih jelasnya mengenai fungsi aplikasi permintaan akses ruangan akan digambarkan pada Gambar 3.6.

3.1.2.3 Rancangan Aplikasi Asosiasi Kartu dengan Akun LDAP

Aplikasi asosiasi kartu dengan akun LDAP digunakan untuk menyimpan UID *smartcard* pengguna ke dalam basisdata *Active Directory*. Hal ini bertujuan agar tidak lagi mengubah isi kartu pengguna dalam melakukan otentikasi nantinya. *Stackholder* yang berperan untuk mengasosiasikan kartu pengguna dengan akun LDAP adalah pegawai akademik. Untuk penjelasan lebih jelas terkait peran yang dapat dilakukan pegawai akademik saat melakukan asosiasi kartu pengguna akan digambarkan pada Gambar 3.6.

Pegawai akademik melakukan login ke sistem aplikasi Xirka menggunakan *username* dan *password* yang terdaftar pada akun LDAP *Active Directory*. Setelah melakukan login, pegawai akademik melakukan *tapping* kartu pengguna ke RFID-reader untuk mengambil data UID dari kartu serta menginputkan username yang berupa NIM/NIK pengguna untuk melakukan asosiasi dengan akun LDAP. Apabila data yang diinputkan cocok maka pegawai akademik dapat melihat data pengguna yang telah terasosiasi dengan UID kartu pengguna.

Pegawai akademik memiliki peran untuk mengasosiasikan pengguna baru dan pengguna lama yang mengalami kehilangan kartu sehingga harus membuat kartu yang baru. Pada prinsipnya setiap orang hanya memiliki 1 identitas unik dari UID-card yang digunakan untuk proses otentikasi. Sehingga jika ada pengguna yang mengalami kehilangan kartu maka UID lama yang telah tersimpan di akun LDAP akan di-*replace* (ditimpa).

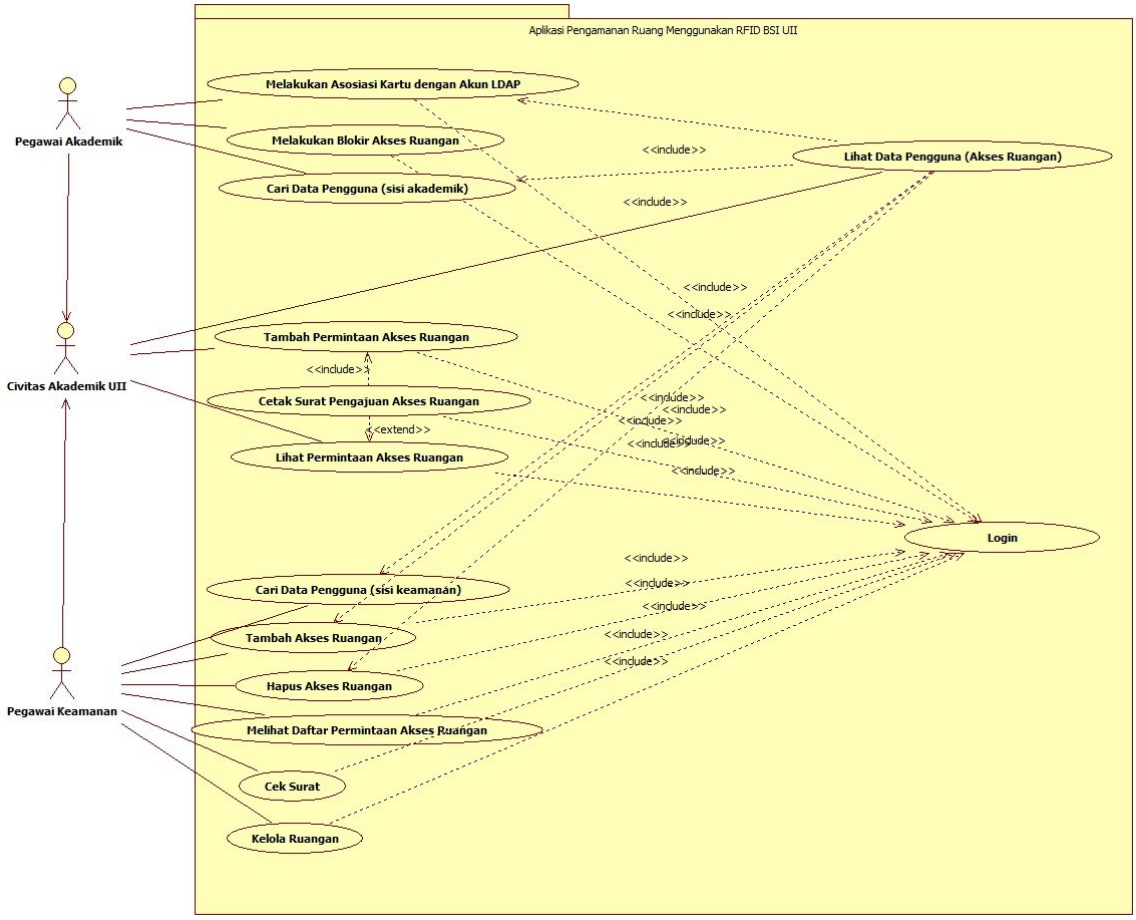
3.1.2.4 Rancangan Aplikasi Blokir Akses Ruangan Pengguna (Kehilangan Kartu)

Selain melakukan asosiasi kartu, pegawai akademik rencananya akan memiliki peran untuk melakukan blokir akses ruangan pengguna jika terjadi kehilangan kartu. Hal ini dilakukan untuk menghapus seluruh akses ruangan pengguna yang telah diberikan pada kartu yang lama (kartu yang hilang) agar tidak disalahgunakan jika kartu tersebut ditemukan oleh pihak lain. Setelah kartu yang lama diblokir, pengguna dapat membuat kartu yang baru dan mengasosiasikan

kembali kartu tersebut ke dalam basis data agar kartu tersebut dapat digunakan kembali untuk mengajukan permintaan akses ruangan.

3.1.2.5 Rancangan Aplikasi Tambah dan Hapus Akses Pengguna Ruangan

Pegawai keamanan (security) memiliki peran untuk menambahkan atau menghapus akses ruangan baik yang akan atau telah diberikan kepada pengguna. Pengguna mendatangi pegawai keamanan (Satpam) terdekat untuk meminta akses ke suatu ruangan tertentu dengan menunjukkan kartu identitas seperti kartu mahasiswa atau kartu pegawai untuk dilakukan penginputan data. Pemberian hak akses dilakukan dengan menambahkan data nomor ruangan ke dalam atribut *roomNumber* melalui aplikasi tersebut sehingga nantinya pengguna bisa terotentikasi dan tervalidasi dari data UID-card dan *roomNumber* yang telah teregistrasi pada akun LDAP. Selain itu pegawai keamanan dapat melihat *list* nomor akses ruangan yang telah diberikan kepada pengguna sehingga apabila pegawai keamanan ingin menghapus suatu akses ruangan terhadap salah satu pengguna dapat melihat dengan pasti akses ruangan yang akan dihapus sehingga tidak terjadi salah hapus akses ruangan nantinya. Untuk lebih jelasnya mengenai peranan yang dapat dilakukan oleh pegawai keamanan dalam menambah dan menghapus akses ruangan pengguna akan digambarkan pada Gambar 3.6.



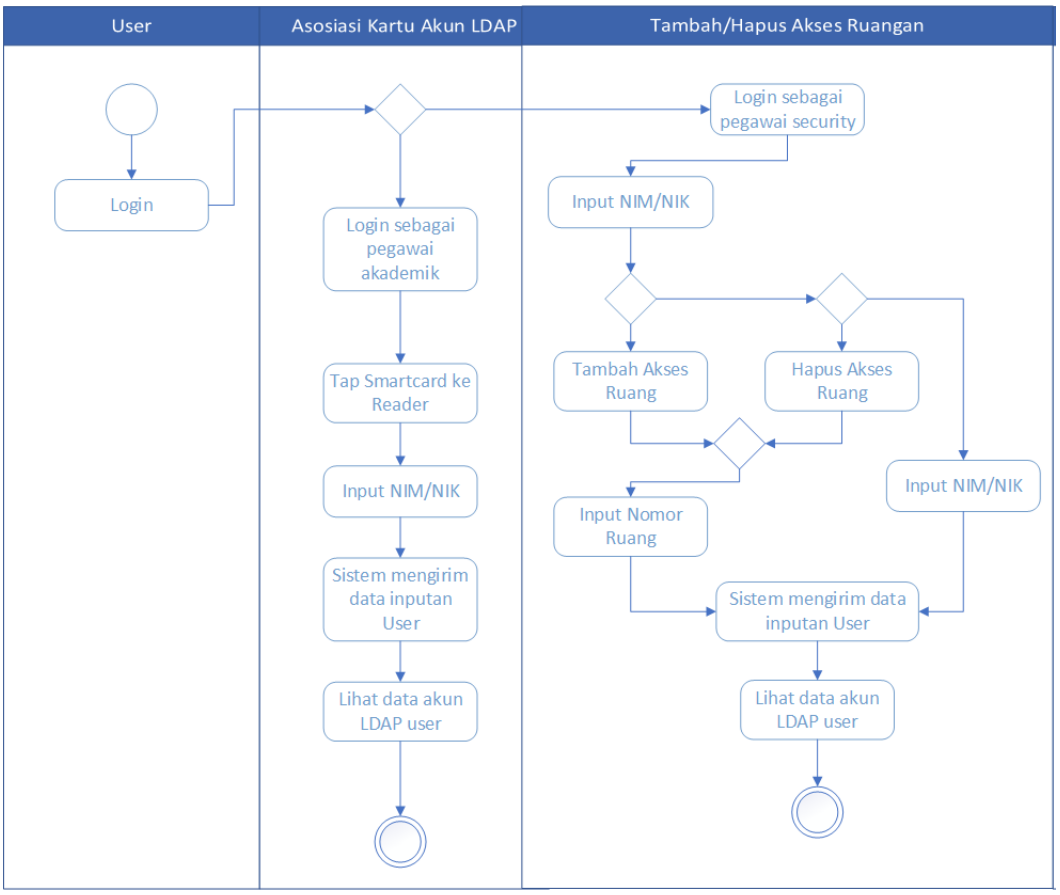
Gambar 3.6 Diagram *Usecase* Aplikasi Pengamanan Ruang Menggunakan RFID di BSI UII

3.1.2.6 Activity Diagram Aplikasi (Kebutuhan Fungsionalitas)

Activity Diagram aplikasi ini akan menjelaskan bagaimana langkah-langkah penggunaan aplikasi asosiasi kartu dengan akun LDAP dan aplikasi tambah serta hapus akses pengguna ruangan yang melibatkan *stackholder* pegawai akademik dan pegawai keamanan. Sistem nantinya akan melakukan pengecekan apakah pengguna yang login teregistrasi sebagai pegawai akademik atau pegawai keamanan karena kedua *stackholder* tersebut memiliki peranan yang berbeda.

Ketika pegawai yang melakukan login teridentifikasi sebagai pegawai akademik, maka sistem akan menampilkan aplikasi asosiasi kartu dengan akun LDAP. Sebaliknya, ketika pegawai yang melakukan login teridentifikasi sebagai

pegawai keamanan (satpam), maka akan diarahkan ke aplikasi tambah/hapus akses ruangan pengguna. Untuk lebih jelasnya akan digambarkan pada activity diagram berikut ini:

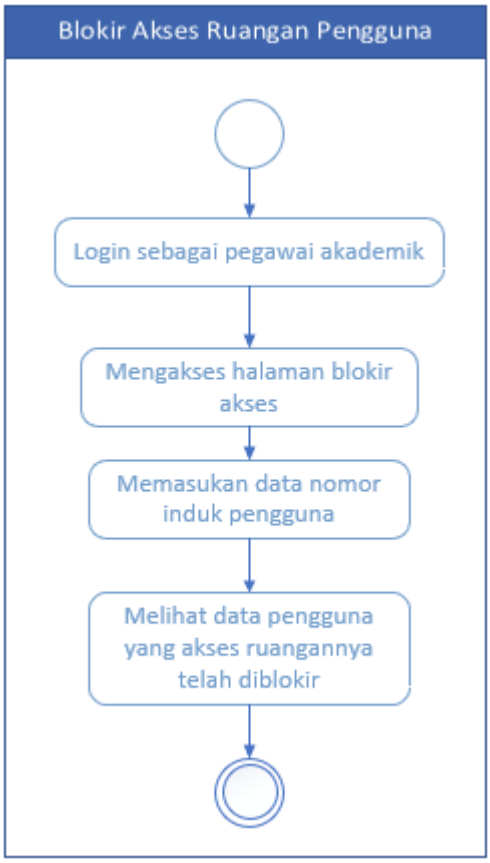


Gambar 3.7 Activity Diagram Aplikasi Asosiasi Kartu Akun LDAP dan Tambah/Hapus Akses Ruangan

Untuk membuat permintaan akses ke sebuah ruangan, pengguna melakukan login ke dalam sistem lalu menambahkan daftar ruangan yang ingin diakses. Setelah itu pengguna dapat mencetak surat pengajuan akses ruangan dan membawanya kepada petugas akademik. Untuk memastikan bahwa pengguna tersebut telah diberi akses ke sebuah ruangan, pengguna tersebut dapat melihatnya pada halaman akses ruangan. Untuk lebih jelasnya akan digambarkan pada diagram aktivitas berikut:

Gambar 3.8 Activity Diagram Aplikasi Permintaan Akses Ruangan

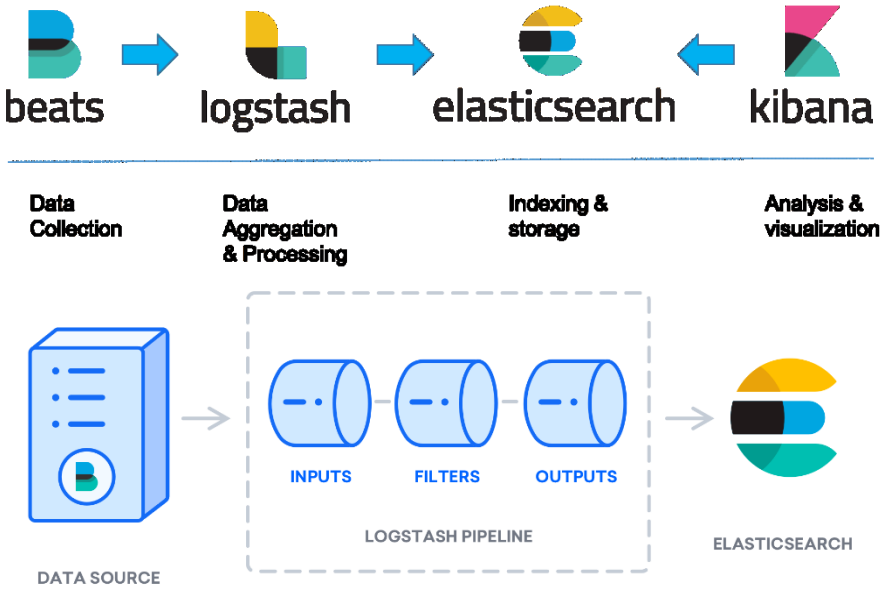
Untuk melakukan blokir akses ruangan pengguna, pegawai akademik rencananya hanya perlu mengakses halaman “Form Hapus Semua Akses Ruangan Pengguna” lalu memasukkan data nomor induk dari pengguna yang ingin diblokir akses ruangannya. Peran pegawai akademik untuk melakukan blokir akses ruangan akan digambarkan pada diagram aktivitas berikut:



Gambar 3.9 Activity Diagram Blokir Akses Ruangan Pengguna

3.1.2.7 Visualisasi Logging dengan 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. Berikut arsitektur sederhana *Elasticsearch, Logstash dan Kibana* (ELK) dalam mengambil log dan melakukan visualisasi log:

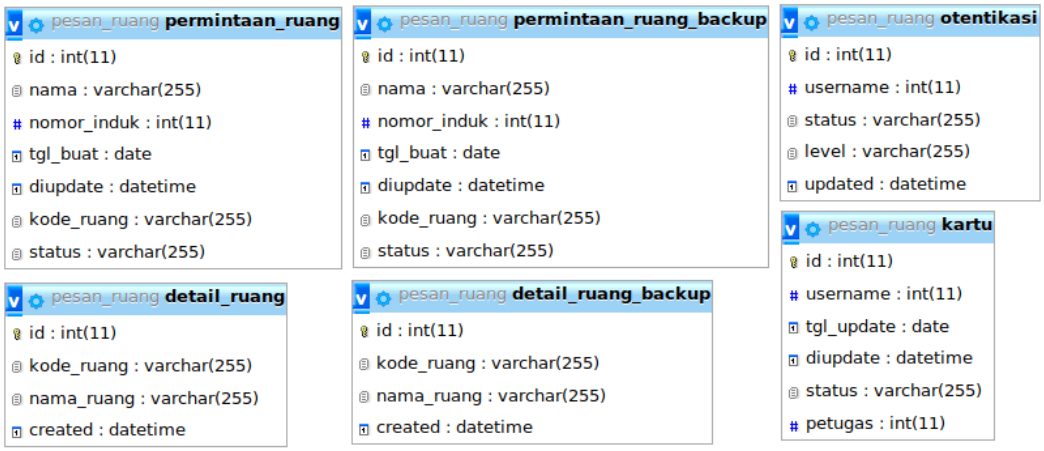


Gambar 3.10 Arsitektur *Elasticsearch, Logstash dan Kibana* (ELK)

Sumber: www.digitalocean.com dan www.logz.io

3.1.2.8 Rancangan Basis Data

Aplikasi web akses kontrol ruang menggunakan dua basis data yang berbeda yaitu MySQL dan Microsoft Active Directory yang berbasis protokol LDAP. Basis data MySQL digunakan untuk menyimpan data ruangan, pengajuan akses ruangan serta log otentikasi ketika pengguna (semua *stackholder*) mengakses aplikasi web tersebut. Pada **Error! Reference source not found.**, rancangan basis data yang d ibuat terdiri dari tabel *otentikasi, permintaan_ruang* dan *detail_ruang*. Secara fungsionalitas, tabel yang digunakan untuk menyimpan data pada aplikasi ini adalah tiga tabel tersebut. Tabel *permintaan_ruang_backup* dan *detail_ruang_backup* hanya digunakan untuk menyimpan data yang telah dihapus dari tabel *permintaan_ruang* dan *detail_ruang.* Hal ini dimaksudkan sebagai langkah pencegahan kehilangan data ketika kita salah menghapus data yang tidak diinginkan. Tabel kartu digunakan untuk menyimpan *record* setiap petugas akademik melakukan asosiasi kartu ke dalam basis data. Untuk lebih jelasnya, rancangan tabel basis data MySQL pada aplikasi web akses kontrol ruang ini digambarkan pada Gambar 3.11 berikut:



Gambar 3.11 Rancangan Basis Data Aplikasi Web Akses Kontrol Ruang

Basis data Microsoft Active Directory yang berbasis protokol LDAP digunakan untuk menyimpan data pengguna seperti *username* dan *password*. Selain itu pada basis data ini juga disimpan beberapa atribut yang digunakan untuk mendukung proses otentikasi dari RFID reader seperti *uid card* dan nomor ruangan. Ketika merancang basis data LDAP ini, penulis menggunakan *phpLDAPadmin* sebagai interface untuk merancang basis data LDAP yang berbasis linux. Namun untuk implementasinya akan disesuaikan dengan basis data Microsoft Active Directory berbasis Windows yang digunakan UII. Basis data LDAP ini juga digunakan untuk membagi hak akses dari masing-masing pengguna yang akan dibagi menjadi sebuah *group* yang terdiri dari group xirka (pengguna umum/civitas akademik), group academik (pegawai akademik), dan group keamanan (pegawai keamanan). Basis data LDAP tidak seperti basis data MySQL yang umumnya berbentuk tabel, melainkan berbentuk hierarki sehingga memudahkan kita dalam melakukan pembagian hak akses dalam bentuk *group*. Untuk lebih jelasnya, rancangan basis data LDAP digambarkan pada Gambar 3.12 berikut:

Gambar 3.12 Rancangan Basis Data Pengguna Akses Kontrol Ruang

3.1.3 Rencana Implementasi

Tahapan selanjutnya yang dilakukan dalam penelitian ini yaitu melakukan implementasi pengembangan sistem dari pemodelan dan rancangan yang telah dibuat sebelumnya. Dashboard akan dibuat menggunakan teknologi berbasis web dan menggunakan web server apache. Implementasi bertujuan untuk mentransformasikan rancangan yang telah dibuat kedalam kode program agar menjadi sebuah aplikasi yang utuh. Kode program aplikasi menggunakan bahasa pemrograman PHP dan python (HTTP server) yang digunakan untuk membuat sistem backend dan komunikasi antara RFID-reader ke LDAP server untuk melakukan otentikasi.

Aplikasi berbasis web ini nantinya hanya akan ditampilkan secara *public* hanya di dalam jaringan internal Universitas Islam Indonesia, sehingga pengguna yang ingin membuat permintaan akses terhadap ruangan harus menggunakan jaringan internet UII. Hal ini dilakukan untuk meningkatkan keamanan karena aplikasi ini berhubungan dengan pemberian hak akses ke sebuah ruangan di lingkungan internal UII. Untuk itu aplikasi web ini akan menggunakan protokol HTTPS (Hypertext Transfer Protocol Secure) yang berjalan pada port 443 dengan melakukan instalasi sertifikat SSL (Secure Socket Layer) agar data yang dikirimkan dan ditampilkan oleh aplikasi web ini dapat dienkripsi dengan baik dan terhindar dari intrusi dari luar.

Sistem pengamanan ruang RFID ini akan diintegrasikan dengan aplikasi kecil atau *backend* yang telah dirancang sebelumnya meliputi aplikasi otentikasi

pengguna, aplikasi asosiasi kartu dengan akun LDAP, aplikasi tambah/hapus akses ruangan pengguna, dan aplikasi permintaan akses ruangan agar menjadi satu kesatuan sistem yang utuh. Untuk melakukan otentikasi rencananya akan menggunakan protokol LDAP yang terintegrasi dengan akun *Active Diretory* di UII. Dalam melakukan audit, rencananya akan menggunakan aplikasi Elasticserach, Logstash, dan Kibana (ELK) untuk melakukan pencatatan aktivitas (log) dan melakukan visualisasi log yang dilakukan oleh sistem.

3.1.4 Rencana Pengujian

Pengujian sistem aplikasi *backend* keamanan ruang menggunakan RFID di BSI UII dapat dilakukan dengan beberapa skenario yang berbeda yaitu skenario pengujian pada aplikasi *backend* dan pengujian RFID-reader.

Skenario pengujian aplikasi *backend* (berbasis web) dilakukan dengan menjalankan dan mencoba semua fitur dari ketiga aplikasi kecil atau *backend* yang telah dibuat yaitu aplikasi otentikasi pengguna termasuk aplikasi pengajuan akses ruangan, aplikasi asosiasi kartu dengan akun LDAP termasuk aplikasi blokir akses ruangan dan aplikasi tambah/hapus akses ruangan pengguna. Hal ini dilakukan guna menguji fungsionalitas sistem tersebut agar dapat berjalan dengan baik dan sesuai dengan harapan pengguna atau *User Acceptance Test* (UAT). Pengujian fungsionalitas menggunakan metode UAT terdiri dari beberapa jenis salah satunya adalah pengujian *Black Box*. Pengujian *Black Box* dilakukan untuk mengetahui fungsionalitas dari setiap aplikasi yang dibangun berhasil atau gagal.

Skenario pengujian RFID-reader dilakukan untuk mengetahui apakah RFID-reader dapat menerima data dari kartu pengguna dan benar-benar melakukan validasi terhadap pengguna yang akan mengakses sebuah ruangan. Harapan yang dihasilkan dari pengujian RFID Reader ada dua yaitu dapat mengecek pengguna valid dan tidak valid serta melakukan pencatatan aktivitas RFID Reader (log) ketika melakukan validasi pengguna. Jika pengguna yang ingin mengakses ruangan tersebut valid, maka akses ruangan diberikan dan pintu akan terbuka. Sebaliknya, jika pengguna tersebut tidak valid maka pintu akan tetap terkunci.