Desain Pengamanan Ganda pada Kontrol Akses Ruang dengan RFID pada Institusi Pendidikan Tinggi

Bayu Aprilananda Sujatmoko
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Yogyakarta
15523090@students.uii.ac.id

Ari Sujarwo
Badan Sistem Informasi,
Universitas Islam Indonesia
Yogyakarta
ari.sujarwo@uii.ac.id

***Abstrak*—Setiap institusi mengembangkan aplikasi dengan menerapkan teknologi RFID sesuai dengan kebutuhan atau masalah yang sedang dihadapi. Teknologi RFID menjadi pilihan karena adanya ID unik pada setiap *tag* yang dapat digunakan untuk identifikasi dan validasi pengguna dengan mencocokkannya terhadap akun yang telah terdaftar di dalam basis data. Di sisi lain RFID bukan merupakan suatu alat yang dapat berdiri sendiri namun RFID akan sangat bermanfaat jika dikembangkan menjadi suatu sistem yang utuh dengan menerapkan berbagai komponen. Pembahasan mengenai permasalahan dan solusi yang digunakan menggunakan teknologi RFID dapat digunakan sebagai acuan dalam penerapan untuk pengamanan ruangan di lokasi penelitian. Dengan banyaknya ruangan, seperti laboratorium atau ruang penting lainnya dan banyaknya pengguna, utilisasi teknologi RFID dirasa lebih tepat karena teknologi RFID relatif murah dan mudah untuk dikembangkan sesuai dengan kebutuhan. Penelitian ini menawarkan pendekatan pengamanan ganda dengan melibatkan beragam pemangku kepentingan dan sekaligus menggali lebih dalam tentang potensi yang dimiliki oleh teknologi RFID pada pengamanan ruangan pada institusi pendidikan tinggi. Fitur yang dimiliki oleh teknologi RFID dengan pengembangan sedikit pada aplikasi backend akan diimplementasikan pada institusi pendidikan tinggi di Yogyakarta.**

Kata kunci—validasi akun, pengamanan ganda, akses ruang, keamanan, RFID

I. PENDAHULUAN

Saat ini hampir semua aktifitas kehidupan manusia saat ini menggunakan teknologi komputer dalam penerapannya. Kebutuhan akan ketersediaannya data secara real time dan kontinu merupakan sebuah kebutuhan yang mendasar dalam kehidupan di era informasi seperti saat ini guna menganalisis data tersebut menjadi sebuah informasi yang bermanfaat [1]. Menurut Few, Dashboard biasa digunakan untuk menampilkan informasi yang berkaitan dengan aktivitas yang dilakukan oleh sebuah sistem dimana dashboard tersebut biasa diwujudukan dalam sebuah web yang memiliki basis data yang memungkinkan untuk diperbaharui secara terus menerus [2]. Kita dapat memantau segala aktivitas melalui dashboard tersebut dan mengambil sebuah keputusan jika diperlukan. Setiap instansi pasti memiliki beberapa ruangan yang memiliki fungsi tertentu misal seperti ruangan divisi keuangan, ruangan manajer, ruangan divisi IT, dan ruang server. Beberapa ruangan tersebut tentunya memiliki keamanan agar tidak sembarang orang bisa memasuki ruangan tersebut dan tentunya hanya orang yang memiliki otorisasi saja yang dapat memasuki ruangan tersebut. Dalam hal ini teknologi informasi sangat dibutuhkan untuk melakukan pengamanan ruang dan memantau siapa saja yang mendapatkan akses untuk memasuki ruangan tersebut melalui dashboard yang dilengkapi teknologi RFID (Radio Frequency Identification).

RFID memiliki 2 bagian yaitu RFID reader dan RFID tag. RFID reader digunakan untuk menerima data yang dipancarkan dari RFID Tag. Kegunaan dari sistem RFID ini adalah untuk mengirimkan data dari tag yang kemudian dibaca oleh RFID reader dan kemudian diproses oleh aplikasi komputer. Data yang dipancarkan dan dikirimkan tadi bisa berisi beragam informasi, seperti ID, informasi lokasi atau informasi lainnya [3]. Data setiap akun tersebut disimpan dalam sebuah sistem yang bernama Active Directory menggunakan teknologi LDAP (Lightweight Directory Access Protocol). LDAP merupakan sebuah protokol untuk mengakses sebuah direktori akun pengguna secara ringan.

Penelitian ini dilakukan di sebuah institusi pendidikan tinggi di Yogyakarta, Indonesia.

II. KAJIAN LITERATUR

A. Penelitian Sebelumnya

Pada institusi tempat penelitian dilakukan terdapat lebih dari 25.000 pengguna yang aktif menggunakan beragam sistem untuk mendukung proses bisnis pendidikan tinggi. Para pengakses ini terdiri dari dosen, mahasiswa, pegawai dan pemangku kepentingan lain seperti orang tua mahasiswa dan tamu. Setiap pengguna diidentifikasi dengan kode yang sebagiannya diwujudkan dalam bentuk kartu identitas.

Pada setiap kartu tertanam di dalamnya RFID Tag yang digunakan untuk melakukan otentikasi menggunakan pada layanan yang telah dilengkapi dengan RFID Reader, seperti sistem mandiri untuk pindai dan cetak. Penelitian pertama pada topik ini dilakukan oleh institusi bersama dengan pengembang RFID reader, yang pada implementasinya mengharuskan untuk mengubah isi dari kartu setiap pengguna dengan menambahkan kode khusus. Akan tetapi, melakukan perubahan data terhadap

25.000 kartu bukanlah perkara sederhana, maka diperlukan penelitian lebih lanjut untuk mengembangkan sistem agar lebih integratif dengan sistem lain yang telah ada sebelumnya.

Arsitektur pada sistem versi pertama masih sangat sederhana. Pengecekan dilakukan dengan melakukan verifikasi eksistensi akun pengguna di dalam Active Directory, dan tidak terdapat proses validasi pengguna lebih mendalam. Dua kelemahan ditemukan pada versi yang pertama yang belum terdapat validasi di dalamnya, yaitu (1) lolosnya semua pengguna yang terdaftar pada Active Directory, sehingga dapat mengakses semua ruangan yang menggunakan teknologi RFID, (2) tidak diaplikasikannya kode ruang pada RFID reader menyebabkan tidak munculnya validitas akses ruang ketika lebih dari satu RFID reader diaplikasikan. Oleh karena itu, pada makalah ini, peneliti berfokus untuk mengembangkan sistem otentikasi yang terbukti mampu melakukan validasi terhadap pengguna yang akan menggunakan akses ruangan tertentu menggunakan teknologi RFID. Selain itu, sistem versi kedua ini diharapkan mampu melakukan pencatatan aktivitas sistem (log), seperti transaksi antara pengguna ke sistem dan pengguna yang mengakses sebuah ruang yang log divisualisasikan menggunakan dashboard untuk mempermudah pemantauan pengguna ruang pada institusi tempat penelitian dilakukan.

B. Autentikasi

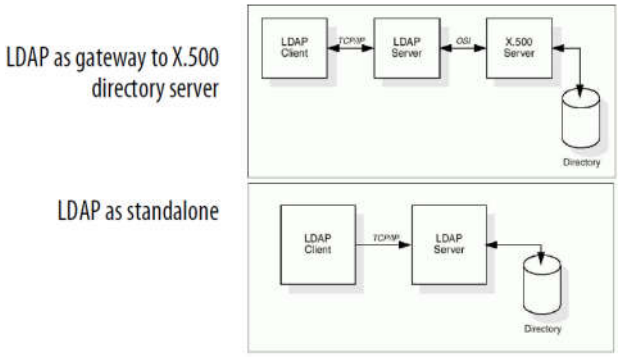
Autentikasi merupakan sebuah proses pengecekan identitas seorang pengguna sistem komunikasi saat melakukan login ke dalam sebuah sistem. Pengguna yang lolos pengecekan identitas adalah pengguna yang resmi terdaftar pada sistem atau orang yang memiliki otoritas pada sebuah sistem. Penggunaan sistem autentikasi diharapkan dapat membentuk sebuah sistem khusus yang dapat dipergunakan oleh orang-orang yang memiliki hak guna [4].

Autentikasi terkadang sering dianggap sama seperti otorisasi, sehingga banyak protokol keamanan yang berdasarkan asumsi tersebut. Padahal, penggunaan istilah autentikasi yang lebih tepat yaitu pembuktian atau pengecekan identitas pengguna sedangkan otorisasi yaitu pengecekan pengguna bahwa pengguna tersebut diberi hak akses atau kuasa untuk melakukan suatu tindakan tertentu di dalam sistem.

C. Teknologi Backend menggunakan Protokol LDAP

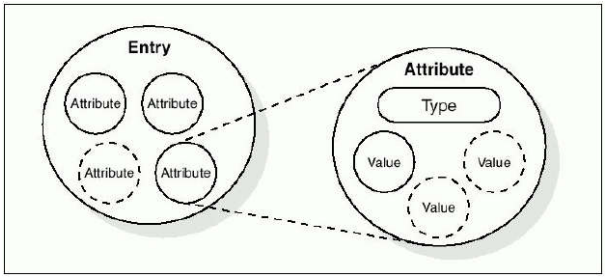
LDAP merupakan singkatan dari Lightweight Directory Access Protocol adalah protokol aplikasi yang digunakan untuk melakukan pengontrolan pada layanan direktori yang berjalan pada protokol TCP/IP (Foundation, 2008). Sesuai namanya, LDAP merupakan sebuah protokol untuk mengakses sebuah direktori akun pengguna secara ringan. Sesuai standar X.500, LDAP mengelola entri direktori ke dalam bentuk hierarki [5]. Direktori Server LDAP dapat digambarkan seperti pada Gambar 1.

LDAP mendefinisikan konten dan format pesan yang dipertukarkan antara LDAP client dan LDAP Server. Pesan tersebut menentukan operasi yang diminta oleh client. LDAP mendefenisikan operasi yang digunakan untuk mengakses dan melakukan modifikasi entri direktori antara lain pencarian sebuah entri yang sesuai dengan kriteria pengguna, menambah entri, menghapus entri, memodifikasi entri, memodifikasi distinguished name atau relative distinguished name dari sebuah entri, dan membandingkan sebuah entri.



Gambar 1. LDAP Directory Server

Struktur LDAP tidak tersusun dari kolom dan baris seperti halnya basis data normal sehingga memudahkan untuk memasukkan detail data dalam bentuk yang terorganisir melainkan seperti sebuah direktori. Direktori merupakan sebuah layanan terstruktur yang disusun secara logis dan hierarkis. LDAP sering digunakan sebagai alat untuk melakukan autentikasi pada berbagai sistem seperti komputer ataupun printer sesuai dengan struktur yang digunakan. LDAP memungkinkan kita untuk mencari suatu organisasi, individu dan juga sumber daya yang lainnya misalnya file atau device di dalam suatu jaringan, seperti ilustrasi pada



Gambar 2. LDAP Information Storage, dipinjam dari (Andri, 2016)

Informasi pada LDAP disimpan dalam sebuah entry seperti pada basis data umumnya, setiap entry memiliki beberapa atribut. Setiap atribut dapat memiliki satu atau lebih nilai. Jika di dalam basis data kita memiliki primary key untuk membedakan suatu entry dengan entry lainnya, maka pada sebuah LDAP kita memiliki Distinguished Name (DN) yang bernilai unik untuk setiap isian.

D. Strategi Pengamanan Ruang

Penelitian yang dilakukan oleh Gyanendra Kumar Verma yang berjudul A Digital Security with Door Lock System Using RFID Technology [6] memaparkan bahwa teknologi RFID dapat diimplementasikan ke dalam berbagai aplikasi keamanan seperti asset tracking, people tracking, inventory detection, dan access control applications. Pada penelitian ini lebih membahas tentang pengimplementasian RFID sebagai salah satu alat keamanan digital yang akan memberikan otentikasi kepada seseorang yang benar-benar memiliki hak

akses. Teknologi RFID dipilih karena teknologi ini tidak memerlukan banyak biaya dalam penerapannya.

Penelitian yang dilakukan oleh Kumar yaitu bagaimana cara mengamankan sebuah ruangan dengan memberikan hak akses kepada seseorang yang benar-benar terotentikasi menggunakan RFID-tag secara real-time disini RFID-tag yang digunakan adalah RFID-tags passive. RFID-tag passive dipilih karena tidak memerlukan baterai, lebih ringan dan tentunya lebih murah dari pada RFID-tag active. Tag passive memiliki respon yang cepat dengan RFID-reader ketika akan menyentuh atau berada dalam jarak beberapa milimeter dari reader. Ringkasan dapat dilihat pada Tabel 1.

Sistem dikelola secara terpusat terkait pengoperasian dan transaksi yang terjadi pada RFID. RFID merupakan suatu sistem yang komperehensif karena tidak bisa berdiri sendiri namun memerlukan beberapa komponen lain dalam pengimplementasiannya yaitu RFID-tag, RFID-reader dan backend system yang dalam penelitian ini dibuat berbasis desktop. Sistem pengamanan pintu ini dikendalikan dan diimplementasikan oleh RFID-reader dimana akan melakukan otentikasi dan validasi pengguna yang akan masuk melalui sebuah pintu.

E. Proses Bisnis Kontrol Akses Ruang

Dalam penelitian yang berjudul Development of an RFID Based Access Control System in the Context of Bangladesh [7] memaparkan tentang bagaimana membuat sistem kontrol akses digital yang bisa digunakan untuk melindungi ruangan atau area dimana hanya pengguna yang terdaftar dan terotentikasi saja yang bisa memasuki ruangan tersebut. Penelitian ini tidak berbeda jauh dengan penelitian yang berjudul A Digital Security with Door Lock System Using RFID Technology karena penelitian ini juga menerapkan teknologi RFID untuk melakukan validasi dan otentikasi pengguna yang akan mengakses sebuah ruangan. Tujuannya yaitu untuk membangun sistem keamanan dengan biaya yang terjangkau dan cocok dengan perspektif negara berkembang seperti Bangladesh.

Sistem ini dibangun diasosiasikan dengan sistem secara terpusat berbasis client-server dan sub sistem untuk memastikan integritas sistem. Asosiasi sub sistem akan melakukan pencatatan aktivitas (log) dan mengelola status check-in dan check-out dari pengguna yang mengunjungi sebuah ruangan. Sistem RFID secara ideal terdiri dari RFID-reader, RFID-tag, dan aplikasi backend yang dilakukan untuk manajemen data. RFID-tag yang digunakan dalam penelitian ini yaitu tag passive karena pengguna yang akan mengakses sebuah ruangan harus mendekati RFID-reader yan terletak didekat pintu tersebut dan menempelkannya paling tidak pada jarak 200 milimeter. Setelah RFID-tag terdeteksi, informasi yang diperoleh diteruskan ke sub-sistem pusat melalui port serial. Server akan melakukan identifikasi data didalam basis data dengan pengguna terdaftar melalui kredensial tertentu. Cross checking dari informasi yang dikirimkan dilakukan secara lokal dan terpusat untuk memastikan otentikasi dan velidasi pengunjung sudah tepat. Pencocokan informasi ini dilakukan untuk membuka kunci pintu magnetik. Perbedaan utama dengan penelitian sebelumnya yaitu sistem ini memberikan hak akses terhadap pengguna suatu ruangan namun admin dari pusat sub sistem dapat membatalkan validitas dari pengguna kapan saja untuk menghindari situasi yang tidak diinginkan. Selain itu pengguna harus mendapatkan akses dari admin sistem yang kemudian akan dikombinasikan untuk proses otentikasi dan validasi menggunakan RFID ketika mengakses sebuah ruangan. Selain itu admin dapat memberikan batasan waktu kepada pengguna untuk mengakses sebuah ruangan sesuai dengan ketentuan yang telah diinisiasikan, kapan pintu terbuka dan tertutup sehingga tidak bisa diakses di sembarang waktu. Sistem ini dibangun dengan aplikasi berbasis web.

Pada penelitian yang berjudul Extension of Genway ECK-03a door control system to work as a part of Elastic based smart building system [8] memaparkan bahwa bagaimana Genway ECK-03A RFID door lock control system atau yang sejenisnya bisa di kolaborasikan dengan sistem smart building berbasis Elastic Stack. Saat ini RFID dengan harga murah memiliki fitur yang sangat sederhana sehingga tidak bisa menghubungkan RFID tersebut ke Building Management System (BMS) sehingga jurnal ini bertujuan untuk mengkolaborasikan ECK-03A dengan Elastic Stack untuk mengintegrasikan perangkat tersebut dengan MQTT server yang berbasis Internet of Things (IoT).

Hal ini berarti teknologi RFID dapat dikombinasikan dengan Elasticsearch yang akan memudahkan kita dalam melakukan pengumpulan data dari log. Untuk melakukan visualisasi data log secara real-time kita bisa menggunakan kibana yang merupakan salah satu bagian dari Elasticstack.

F. Tipikal Arsitektur Sistem

RFID pada dasarnya merupakan teknologi yang relatif terjangkau dan dapat diaplikasikan menggunakan transmisi jaringan wireless. Dengan menggunakan RFID yang terhubung ke jaringan wireless berbagai macam objek dapat dilakukan identifikasi seperti lokasi atau informasi individu yang ditandai dengan ID unik yang terdapat pada RFID-tag yang telah tertanam pada kartu pengguna. RFID merupakan suatu sistem yang komrehensif yang secara tipikal terdiri dari tiga elemen dasar yaitu RFID-tag (transponder), RFID-reader (transreceiver) dan sistem aplikasi backend atau basis data, yang didukung oleh komputer dan jaringan internet sehingga RFID dapat memiliki fungsi seperti manajemen, kontrol pengguna, pencatat transaksi dan maintenance record pengguna [6].

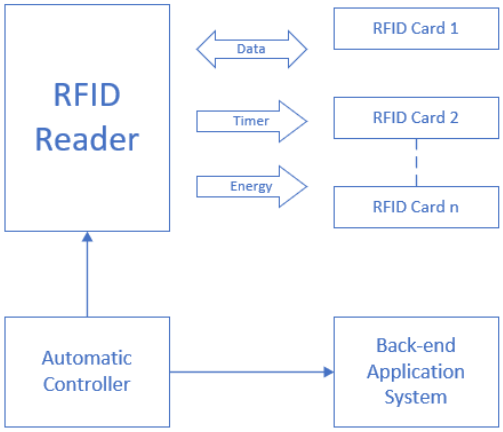
Sistem pengamanan ruang yang memanfaatkan teknologi RFID digunakan untuk melakukan otentikasi dan validasi pengguna ketika akan membuka pintu secara otomatis. Hal ini tentunya akan melakukan pencatatan check-in dan check-out pengguna ketika mengakses sebuah ruangan. Otentikasi dan validasi ini dilakukan dengan cara mencocokkan informasi yang terdapat di dalam RFID-tag pengguna dengan data akun pengguna di basis data. Sehingga pengguna yang benar-benar terdaftar yang akan memiliki akses untuk mengakses sebuah ruangan. RFID akan memberi sinyal ke sistem doorlock apabila pengguna terotentikasi untuk membuka pintu.

Dalam hal ini RFID-tag yang cocok digunakan adalah tag passive dikarenakan tag tersebut tidak menggunakan baterai karena memanfaatkan energi yang berasal dari RFID-reader

serta keunggulan utamanya adalah harganya yang murah dan ukurannya yang kecil sehingga mudah digunakan [6]. Secara umum tipikal sistem arsitektur RFID digambarkan seperti Gambar 3.

TABEL I. TABEL PERBANDINGAN PENERAPAN RFID

No	Nama Penulis	Judul Tesis	Tujuan	Solusi
1	Verma & Tripathi, 2010	A Digital Security with Door Lock System Using RFID Technology	Mengamankan ruang dan melakukan otentikasi atau hak akses secara langsung ke pengguna serta melakukan pencatatan aktivitas pengguna ruangan.	Menggunakan teknologi RFID untuk melakukan otentikasi dan validasi pengguna yang dikombinasikan dengan backend aplikasi yang mampu mengintegrasikan antara RFID-reader dengan basis data akun pengguna.
	Shafin et al., 2015	Development of an RFID Based Access Control System in the Context of Bangladesh	Mengamankan ruang dengan membuat sistem kontrol akses pengguna yang dapat memberi izin pengguna untuk mengakses sebuah ruangan, misal berapa lama	Menggunakan teknologi RFID untuk melakukan otentikasi pengguna ruangan yang diintegrasikan dengan basisdata akun pengguna melalui aplikasi backend yang dikembangkan.
	Bajer, 2017	Extension of Genway ECK-03a door control system to work as a part of Elastic based smart building system	pengguna dapat mengakses ruangan tersebut, mencatat aktivitas pengguna dan memvisualisasikan aktivitas pengguna tersebut (log)	Mengkombinasikan teknologi RFID dengan kakas Elastic Stack dengan mengembangkan aplikasi backend



Gambar 3. Tipikal implementasi sistem RFID, gambar dipinjam dari (Verma & Tripathi, 2010)

III. KEBUTUHAN SISTEM

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 pada lokasi penelitian. 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. Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan untuk membangun sistem aplikasi backend keamanan ruang membutuhkan 1 buah server dengan sistem operasi Linux/Ubuntu, RFID-tag (kartu pengguna/smartcard), RFID-reader, kartu master editor, dan kartu master. Gambar 3 menunjukkan perangkat keras yang diperlukan.

Gambar 4. Kebutuhan perangkat keras, dari kiri ke kanan: RFID-reader, RFID-tag (smartcard), kartu master editor, dan kartu master.

B. Kebutuhan Fungsional

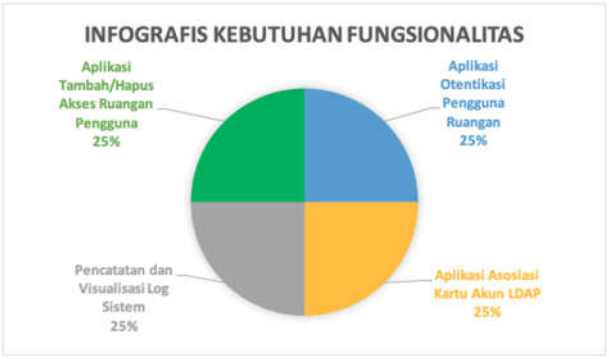
Terdapat empat kebutuhan fungsionalitas utama yang dikembangkan di dalam penelitian ini yaitu otentikasi pengguna ruangan, aplikasi asosiasi kartu dengan akun LDAP, aplikasi tambah dan hapus akses pengguna ruangan, dan pencatatan serta visualisasi pencatatan aktivitas sistem atau log.

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 akademika.

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 satuan pengamanan (Satpam).

Kebutuhan fungsionalitas yang terakhir yaitu pencatatan dan visualisasi aktivitas sistem (log). Sistem diharapkan memiliki kemampuan untuk mencatat transaksi yang terjadi selama sistem digunakan. Untuk lebih jelasnya kebutuhan fungsionalitas sistem keamanan ruang menggunakan RFID digambarkan pada Gambar 4.



Gambar 5. Infografis Kebutuhan Fungsionalitas Sistem Keamanan Ruang Menggunakan RFID

Peneliti memberikan persentase bobot prioritas yang sama pada setiap fungsionalitas karena masing-masing dari fungsionalitas tersebut memiliki peranan yang sama pentingnya terhadap proses bisnis yang berjalan di sistem keamanan ruang menggunakan RFID dan setiap fungsionalitas memiliki keterkaitan antara satu dengan yang lainnya.

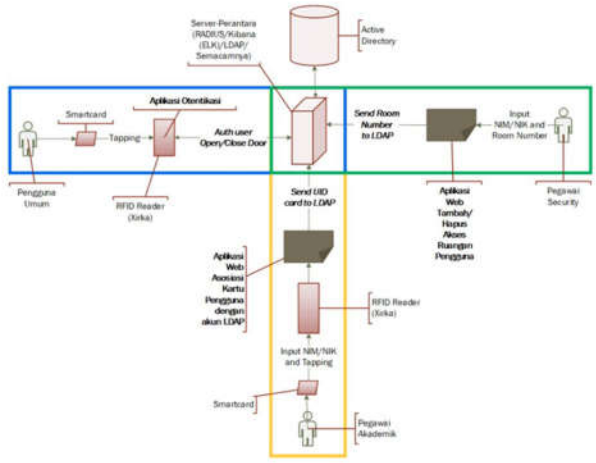
Selain 4 kebutuhan utama fungsionalitas di atas, dibutuhkan satu kebutuhan tambahan yang berguna untuk mendukung jalannya proses bisnis saat pengguna ingin mengajukan akses sebuah ruangan. Oleh karena itu, dibuat sebuah sistem sederhana yang digunakan oleh pengguna untuk membuat daftar permintaan akses 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.

IV. ARSITEKTUR SISTEM DENGAN PENGAMANAN GANDA

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 [9]. 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 [6].

Berdasarkan paparan di atas, peneliti 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 institusi. 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. Rancangan arsitektur sistem keamanan ruang menggunakan RFID dapat dilihat pada Gambar 6.



Gambar 6. Rancangan Arsitektur Sistem Keamanan Ruang Menggunakan RFID

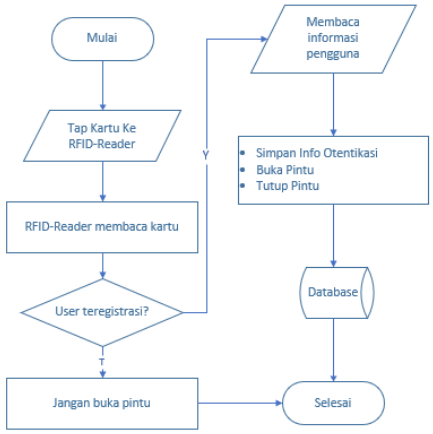
Berdasarkan rancangan sistem tersebut terdapat tiga pemangku kepentingan yang berperan dalam menggunakan sistem yaitu pengguna secara umum, pegawai akademik, dan pegawai security. Pengguna secara umum merupakan orang yang akan melakukan akses sebuah ruangan dengan menyentuhkan smartcard ke RFID-reader untuk melakukan otentikasi yang berkaitan dengan seluruh civitas akademika.

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 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.

A. 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. Di sisi 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, 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 dapat dilihat pada Gambar 7.



Gambar 7. Diagram Alur Otentikasi Pengguna saat Akses Ruangan

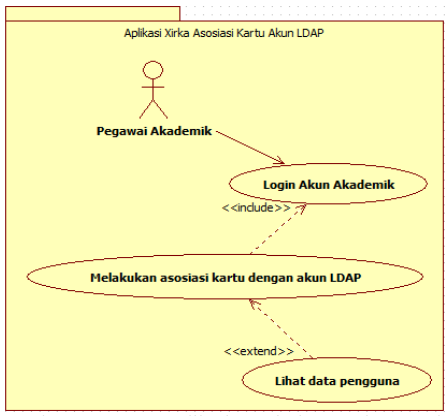
B. Rancangan Sistem Keamanan Ganda

Aplikasi asosiasi kartu dengan akun LDAP berguna untuk menyimpan UID smartcard pengguna ke dalam basisdata Active Directory. Hal ini bertujuan agar tidak lagi mengubah isi kartu pengguna dalam melakukan otentikasi nantinya. Pengamanan ganda diwujudkan melalui peran berbagai pemangku kepentingan: pegawai unit akademik sebagai penerbit kartu sekaligus berperan untuk mengasosiasikan kartu pengguna dengan akun LDAP (Gambar 8), serta pegawai satuan keamanan yang melakukan verifikasi dan persetujuan permintaan akses.

Pegawai akademik melakukan login ke sistem aplikasi 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 membutuhkan penggantian kartu. Pada prinsipnya setiap orang hanya

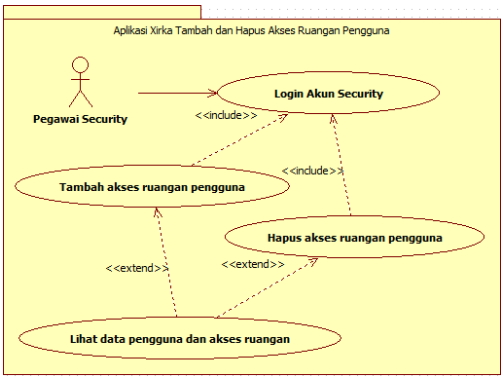
memiliki 1 identitas unik dari UID-card yang digunakan untuk proses otentikasi. Sehingga jika ada pengguna yang mengalami kehilangan kartu maka UID lama yang telah tersimpan di akun LDAP akan ditimpa.



Gambar 8. Usecase Aplikasi Asosiasi Kartu dengan Akun LDAP

C. Rancangan Aplikasi Tambah dan Hapus Akses Pengguna Ruangan

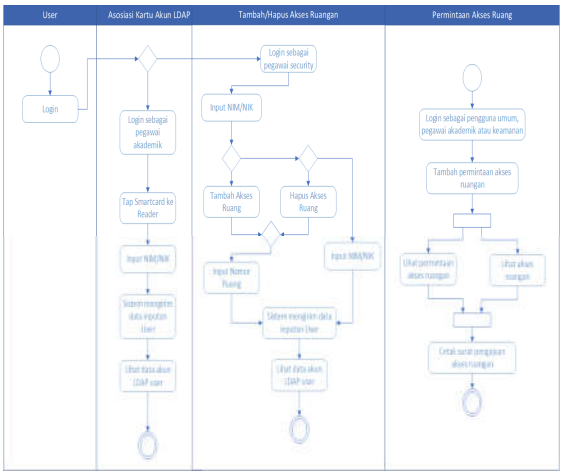
Pegawai keamanan (security) memiliki peran untuk menambahkan atau menghapus akses ruangan baik yang akan atau telah diberikan kepada pengguna. Pengguna mendatangi pegawai keamanan (Satpam) terdekat untuk meminta akses ke suatu ruangan tertentu dengan menunjukkan kartu identitas seperti kartu mahasiswa 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 (Gambar 9).



Gambar 9. Usecase Aplikasi Tambah dan Hapus Akses Pengguna Ruangan

D. Activity Diagram Aplikasi (Kebutuhan Fungsionalitas)

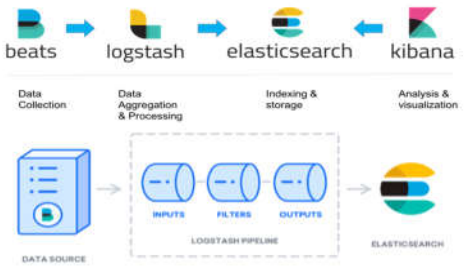
Activity Diagram aplikasi ini akan menjelaskan bagaimana langkah-langkah penggunaan aplikasi asosiasi kartu dengan akun LDAP dan aplikasi tambah serta hapus akses pengguna ruangan yang melibatkan stackholder pegawai akademik dan pegawai keamanan. Sistem nantinya akan melakukan pengecekan apakah pengguna 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 (Gambar 10).



Gambar 10. Activity Diagram Aplikasi Asosiasi Kartu Akun LDAP dan Tambah/Hapus Akses Ruangan

E. Visualisasi Logging dengan Kibana

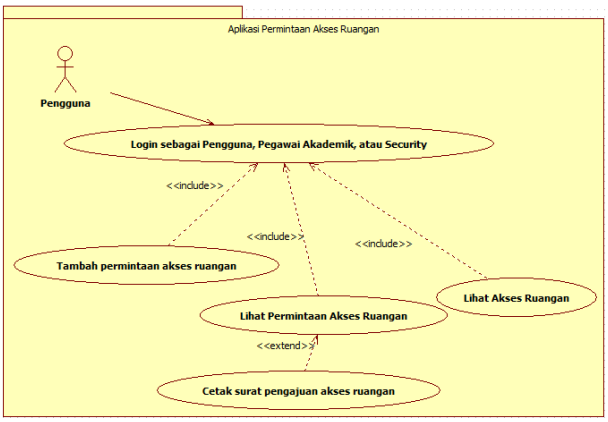
Kibana adalah sebuah antarmuka yang digunakan untuk melakukan visualisasi dari log. Kibana memerlukan Elasticsearch dan Logstash. Logstash bertugas untuk mengambil log dari hasil logging yang dilakukan oleh protokol LDAP atau web server Apache sedangkan Elasticsearch bertugas untuk melakukan pengumpulan data dari log yang selanjutnya data log tersebut digunakan Kibana untuk divisualisasikan (Gambar 11).



Gambar 11. Arsitektur Elasticsearch, Logstash dan Kibana (ELK), gambar dipinjam dari www.digitalocean.com

F. 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 akademika. 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 (Gambar 12).



Gambar 12. Usecase Aplikasi Permintaan 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 (Gambar 13).

Gambar 13. Activity Diagram Aplikasi Permintaan Akses Ruangan

V. PROTOTIPE

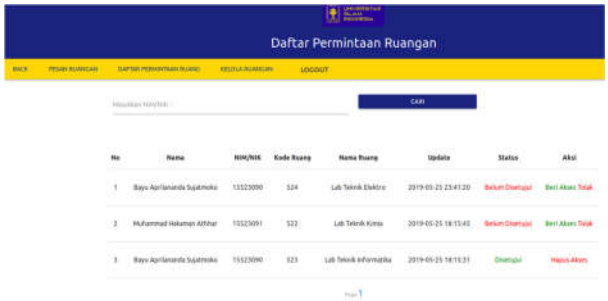
Pada Gambar 14 ditunjukkan sebuah daftar pengajuan akses ruangan. Pada bagian ini pengguna wajib membuat permintaan akses ruangan untuk mendapatkan akses ke sebuah ruangan.

Gambar 14. Daftar Pengajuan akses Ruangan

Pada Gambar 15 ditunjukkan sebuah form yang berfungsi untuk melakukan asosiasi ID kartu ke dalam basisdata. Pada bagian ini dilakukan oleh pegawai akademik. Asosiasi kartu bertujuan untuk mendaftarkan pengguna agar dapat menggunakan sebuah ruangan.

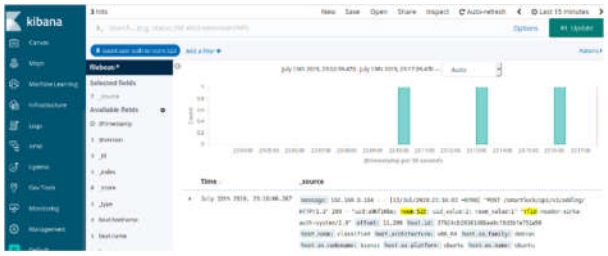
Gambar 15. Form Asosiasi Kartu ke dalam Basis Data

Pada Gambar 16 ditunjukkan sebuah daftar permintaan akses ruangan. Pada bagian ini yang memiliki peran adalah pegawai keamanan (security). Pegawai keamanan memiliki wewenang untuk memberikan akses ruangan kepada pengguna yang digunakan untuk validasi di RFID Reader nantinya. Pegawai keamanan dapat menolak permintaan akses ruangan jika pengguna terindikasi bukan merupakan civitas akademika dari institusi di penelitian ini.



Gambar 16. Daftar Permintaan Akses Ruangan

Pada Gambar 17 ditunjukkan sebuah gambar visualisasi log dalam bentuk grafik. Log ini mencatat jumlah pengguna yang mengakses sebuah ruangan dengan menggunakan kakas kibana.



Gambar 17. Visualisasi Log Pengguna yang Mengakses Ruangan

Pada Gambar 18 ditunjukkan sebuah gambar dari *terminal* sebuah server yang menunjukkan kondisi valid atau tidak nya pengguna melalui otentikasi RFID Reader. Pengguna akan valid selama *output* di terminal tersebut tidak nol.

Gambar 18. Validasi Pengguna Melalui RFID Reader

Pada Gambar 19 ditunjukkan sebuah gambar yang berisi informasi umum dari pengguna dan daftar ruangan yang bisa diakses oleh pengguna tersebut.

Gambar 19. Daftar Akses Ruangan Pengguna

Pada Gambar 20 ditunjukkan sebuah gambar surat yang berisi daftar permintaan akses ruangan yang telah dibuat oleh pengguna. Surat ini digunakan untuk memvalidasi pengguna apakah termasuk civitas akademika institusi di penelitian ini atau tidak yang dilakukan oleh pegawai keamanan sebelum memberikan akses ruangan.

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

Petugas Keamanan UII

Yang Mengajukan Akses Ruangan

NIK.

Nomor Induk.

Gambar 20. Surat Pengajuan Akses Ruangan

VI. KESIMPULAN

Sistem pengamanan ganda pada ruang dengan memanfaatkan teknologi RFID telah didesain dengan pendekatan multi-pemangku kepentingan, dengan mempertimbangkan kebutuhan fungsional dan perangkat keras untuk memenuhi kebutuhan yang masif pada institusi pendidikan tinggi. Penelitian ini merupakan sebuah pendekatan yang selanjutnya diikuti dengan proses pembuatan purwarupa dan pengujian.

Pembahasan mengenai permasalahan dan solusi yang digunakan menggunakan teknologi RFID dapat digunakan sebagai acuan dalam penerapan untuk pengamanan ruangan yang ada di institusi penelitian ini. Dengan banyaknya ruangan, seperti laboratorium atau ruang penting lainnya dan banyaknya pengguna di institusi penelitian ini, penggunaan teknologi RFID dirasa lebih tepat karena teknologi RFID relatif murah, mudah untuk dikembangkan sesuai dengan kebutuhan, serta RFID-tag yang memiliki ID unik. RFID-tag unik ini akan sangat membantu dalam proses pengembangan aplikasi untuk melakukan validasi dan otentikasi pengguna yang akan menggunakan ruangan.

Penelitian ini akan menggali lebih dalam tentang potensi yang dimiliki oleh teknologi RFID jika digunakan untuk melakukan pengamanan ruangan diskala universitas. Fitur yang dimiliki oleh teknologi RFID dengan pengembangan sedikit pada aplikasi *backend* akan diimplementasikan untuk mengamankan sebuah ruangan di institusi penelitian ini.

Untuk saat ini, kebutuhan yang telah dipenuhi dari penelitian ini yaitu adanya aplikasi *backend* yang digunakan sebagai akses kontrol terhadap ruangan dan pencatatan log yang divisualisasikan ke dalam bentuk grafik. Sistem ini belum mampu melakukan penghitungan waktu berapa lama pengguna mengakses sebuah ruangan. Harapan ke depan untuk versi selanjutnya, sistem ini mampu menghitung waktu pengguna ketika mengakses sebuah ruangan dan memberi batasan waktu saat mengakses ruangan tersebut.

REFERENSI

[1] N. Martin, J. Bergs, D. Eerdekens, B. Depaire, and S. Verelst, "Developing an emergency department crowding dashboard: A design science approach," Int. Emerg. Nurs., vol. 39, pp. 68–76, 2018.

[2] S. Few, "Information dashboard design : displaying data for at-a-glance monitoring," Inf. dashboard Des. displaying data at-a-glance Monit., p. 246, 2013.

[3] S. Budiharjo and S. Milah, "Keamanan Pintu Ruangan Dengan Rfid Dan Password Menggunakan Arduino Uno," J. ICT Penelit. dan Penerapan Teknol., pp. 28–34, 2014.

[4] A. Sujarwo, "Implementasi Network Storage dan Internet gateway Menggunakan Autentikasi OpenLDAP," in Seminar Nasional Aplikasi teknologi Informasi 2010, 2010, p. 25.

[5] M. A. Setiawan, "Directory Services," Yogyakarta: Informatika UII, 2016.

[6] G. K. Verma and P. Tripathi, "A Digital Security System with Door Lock System Using RFID Technology," Int. J. Comput. Appl., vol. 5, no. 11, pp. 6–8, 2010.

[7] M. K. Shafin et al., "Development of an RFID based access control system in the context of Bangladesh," ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst., no. March, 2015.

[8] M. Bajer, "Extension of Genway ECK-03A door control system to work as a part of Elastic based smart building system," no. October, 2017.

[9] M. R. Rieback, G. N. Gaydadjiev, B. Crispo, R. F. H. Hofman, and A. S. Tanenbaum, "A Platform for RFID Security and Privacy Administration," Auditing, pp. 89–102, 2006.