

BAB II

KAJIAN PUSTAKA

2.1 Landasan Teori

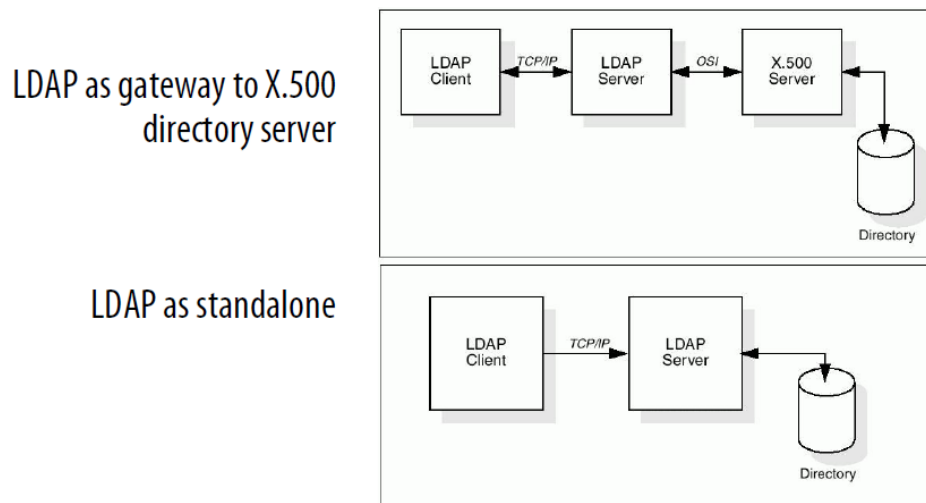
2.1.1 Autentikasi

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 (Sujarwo, 2010).

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.

2.1.2 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 (Andri, 2016). Direktori Server LDAP dapat digambarkan seperti Gambar 2.1 berikut:



Gambar 2.1 LDAP Directory Server

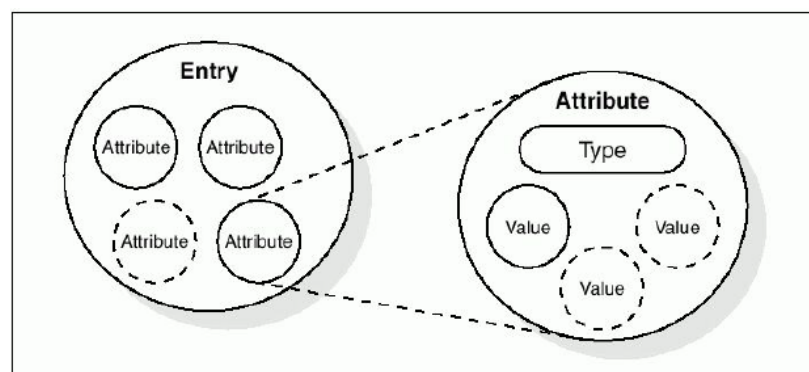
Sumber: (Andri, 2016)

LDAP menggunakan model *client-server* dimana *client* akan mengirimkan sebuah data berupa *identifier* ke *server* menggunakan protokol TCP/IP dan server tersebut akan mencari data tersebut pada sebuah DIT (Directory Information Tree) yang digambarkan pada Gambar 2.3. Jika data yang dicari ditemukan maka data tersebut akan dikirimkan kepada *client*, namun jika tidak maka hasilnya akan diteruskan ke *server* lain yang menyimpan data yang sedang kita cari. LDAP mendefinisikan konten dan format pesan yang dipertukarkan antara LDAP *client* dan LDAP Server. Pesan tersebut menentukan operasi yang diminta oleh *client*. LDAP mendefinisikan 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. Tahapan interaksi umum antara LDAP *client* dan LDAP Server adalah sebagai berikut:

1. *Binding* yaitu client membuat sesi dengan server LDAP. Client menentukan nama host atau alamat IP dan nomor port TCP/IP dimana server LDAP melakukan *Listening port*. Client mengotentikasi sendiri dengan Server LDAP.

2. *Client* kemudian melakukan operasi pada data direktori. LDAP menawarkan kemampuan membaca dan memperbarui direktori. Hal ini memungkinkan informasi direktori untuk dikelola dengan baik.
3. *Unbinding* yaitu ketika client telah selesai membuat request dan menutup sesi dengan server.

Dalam perkembangannya, LDAP memanfaatkan *Domain Name System* untuk mendukung penamaan pada struktur direktori. LDAP dapat menggambarkan organisasi, pengguna, komputer, printer, atau hal lain sesuai dengan struktur yang diberikan pada LDAP. 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* ataupun *device* didalam suatu jaringan. Berikut adalah diagram yang menggambarkan informasi penyimpanan LDAP :



Gambar 2.2 LDAP Information Storage

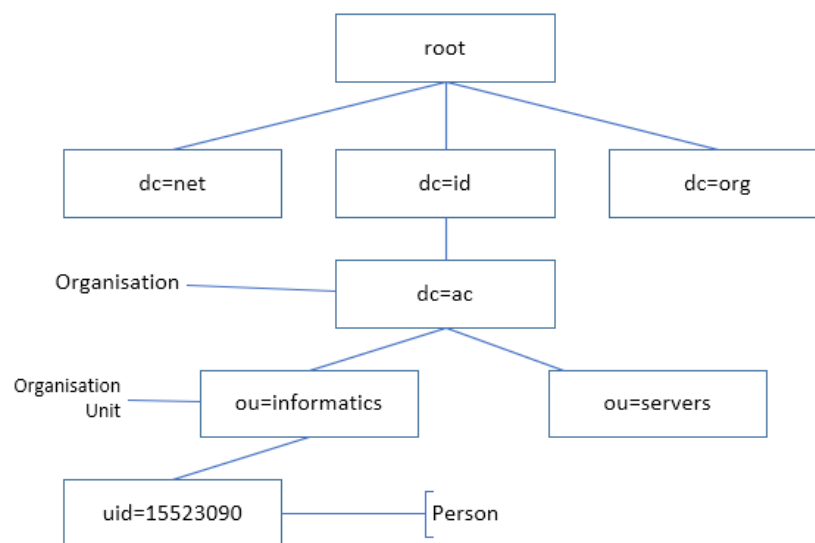
Sumber : (Andri, 2016)

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 *entry*. DN didapat dengan merunut lokasi *entry* hingga akar *hierarki*, contohnya sebagai berikut :

```
dn: uid=15523090,ou=informatics,dc=ac,dc=id
uid: 15523090
cn: bayusujatmoko
mail: bayusujatmoko@gmail.com
objectClass: person
```

Dari contoh diatas, dapat kita lihat bahwa DN merupakan hasil dari pengurutan sumber hingga akar hierarki (root). Atribut uid (user id), cn (common name), *mail* dan *objectClass* merupakan atribut yang dimiliki *entry* tersebut. *Object Class* yaitu kelas-kelas yang diturunkan sifatnya oleh sebuah *entry* dan sebuah *entry* dapat menurunkan lebih dari satu *objectClass*. Berikut adalah contoh struktur DIT (Directory Information Tree) :



Gambar 2.3 Directory Information Tree

Selain DN, sebuah *entry* juga memiliki RDN (Relative Distinguished Name). RDN hanya membedakan suatu *entry* dengan *entry* lainnya di bawah sebuah percabangan yang sama. Misalnya untuk contoh diatas, pada *ou=informatics*, 15523090 memiliki RDN *uid=15523090* untuk membedakannya dengan *uid=15523091*. Singkatnya DN adalah nama lengkap sedangkan RDN adalah nama file dalam folder. DN dapat berubah sesuai dengan struktur hierarki. Penamaan atribut LDAP akan dituliskan pada Tabel 2.1 berikut :

Tabel 2.1 Penamaan Atribut pada LDAP

Type Atribut	String
CommonName	CN
LocalityName	L
StateorProvinceName	ST
OrganizationName	O
OrganizationalUnitName	OU
CountryName	C
StreetAddress	STREET
domainComponent	DC
Userid	UID

2.1.3 RFID

Teknologi RFID (Radio Frequency Identification) merupakan sebuah teknologi yang digunakan untuk identifikasi dan verifikasi menggunakan gelombang radio yang tidak membutuhkan kontak langsung antara objek dengan pembacanya (Prakananda, 2012). RFID merupakan teknologi yang dapat melakukan identifikasi beberapa objek sekaligus tanpa adanya kontak fisik secara langsung. Teknologi RFID memerlukan tiga komponen utama yaitu RFID Tag yang bebrbentuk *chip* yang tipis dan kecil, RFID *Reader* yang digunakan untuk membaca data pada Tag, dan aplikasi yang melakukan pemrosesan data yang didapat melalui *Reader*. Komponen-komponen yang terdapat pada RFID yaitu:

1. RFID Tag, berdasarkan jenis tagnya, RFID dibedakan menjadi dua yaitu:
 - a. Aktif
Tag ini menggunakan tenaga baterai serta memiliki jarak baca yang lebih jauh, mulai dari 20 meter hingga 300 meter. Tag ini tidak memantulkan sinyal radio, melainkan mengirim sinyal radio tersebut.
 - b. Pasif
Tag Pasif yaitu tag konvensional yang memantulkan sinyal yang diberikan oleh *reader*. Jarak baca tag pasif relatif pendek. Tag ini memiliki bentuk seperti lembaran chip sehingga mudah diaplikasikan di berbagai media. Tag pasif dapat beroperasi pada *low*, *high*, dan *ultra-high frequency*.
2. RFID Reader
RFID Reader digunakan untuk mengirim dan menerima sinyal dari tag. RFID Reader dapat membaca tag secara kasar (RAW) dan tidak memiliki kemampuan komputasi.
3. Middleware
Middleware merupakan aplikasi yang menerima data dari reader dan mengolahnya agar sesuai dengan kebutuhan sistem. Middleware dapat melakukan salah satu pekerjaan seperti memfilter RAW data dan memonitoring keadaan *reader*.

Ada beberapa hal yang perlu dipertimbangkan dalam mengimplementasikan teknologi RFID, seperti yang dijelaskan tabel Tabel 2.2 berikut:

Tabel 2.2 Aspek yang perlu dipertimbangkan dalam penerapan RFID

No	Aspek	Keterangan
1	Jenis tag	Pemilihan antara tag aktif dan pasif. Hal ini mempengaruhi jarak baca dan keamanan data yang tersimpan dalam tag
2	Jarak baca	Perkiraan jarak yang dibutuhkan pada saat penggunaan. Hal ini akan mempengaruhi aksesibilitas tag.
3	Proteksi fisik terhadap tag	Proteksi fisik dilakukan agar tag tidak rusak dan tidak dapat dibaca pada saat tidak digunakan. Hal ini dilakukan untuk mencegah pencurian data pada tag. Cara proteksi dapat menggunakan tempat penyimpanan seperti ditanamkan didalam kartu.
4	Penyimpanan data	Tag dapat menyimpan nomor identifikasi (UID) dengan database yang terpisah pada lokasi yang aman atau tag juga perlu menyimpan data lainnya dalam memory.
5	Proteksi fisik terhadap reader	Proteksi fisik terhadap reader dilakukan agar reader aman dari segala tindakan yang memungkinkan akan menyebabkan reader rusak. Hal ini biasa terjadi ketika ada seseorang yang ingin mendapatkan akses dengan cara yang ilegal.
6	Enkripsi UID tag kartu	RFID Reader melakukan enkripsi <i>uid</i> tag kartu saat data <i>uid</i> tag dikirimkan ke basis data.

Sumber: (Prakananda, 2012)

2.2 Penerapan RFID di Berbagai Bidang

2.2.1 Internet of Things

Saat ini hampir semua perangkat elektronik dapat terhubung ke internet tidak terkecuali RFID. Dalam jurnal yang berjudul *Building the Internet of Things Using RFID* (Welbourne et al., 2009) di Universitas Washington, memaparkan bahwa RFID dapat dikembangkan ke dalam berbagai tools dengan memanfaatkan jaringan komputer sehingga terbentuk sebuah ekosistem *Internet of Things* (IoT) disana. Peneliti tersebut mengembangkan beberapa tools berbasis web, tools pada level pengguna dan desain aplikasi yang bertujuan untuk mendukung pengguna dalam memfasilitasi manajerial dan kontrol data personal RFID serta pengaturan privasi. Jumlah informasi yang tersimpan di dalam triliunan RFID tags saat ini tentunya akan memberikan efek yang cukup besar jika kita memanfaatkannya dalam kegiatan sehari-hari contohnya kita bisa mentransformasikan RFID tersebut dan

mengaplikasikan dengan kegiatan fisik seperti bisnis dalam bidang pengamanan pintu, data personal dan sebagainya. Perkembangan RFID-tags *passive* yang begitu cepat membuat inovasi RFID di bidang IoT semakin berkembang.

Ada beberapa tools yang dikembangkan dalam penelitian di jurnal ini. Yang pertama adalah tools pada level pembuat, peneliti tersebut membuat sebuah aplikasi untuk mengasosiasikan objek tag secara manual. Hal ini dilakukan karena sebagian besar objek belum disematkan kedalam tag yang dibuat dan metadata yang dimuat oleh pabrik ke dalam tag tidak memiliki makna untuk data personal. Tujuannya utamanya adalah pengguna dapat memilih RFID tag dan mengaitkannya dengan objek yang dibuat. RFID Reader melakukan koneksi ke server lalu aplikasi ini akan mendeteksi RFID tag dan menghasilkan tag-red event (TRE) per tag antenna per detik dengan skema (ID tag, ID antenna, waktu) dimana data tersebut disimpan di dalam SQL Server.

Alat atau tools berikutnya adalah pada level pengguna. Di dalam jurnal ini peneliti tersebut membuat aplikasi untuk melakukan transformasi low-level data RFID ke dalam higher-level data secara langsung dengan mendefinisikan metadata dan mengasosiasikannya dengan tag dan antenna. Aplikasi tersebut bernama Tag Manager dan berbasis web untuk membuat dan *manage* metadata pada tag pengguna dan data personal. Contohnya pengguna baru dapat melakukan pendaftaran beberapa data personal pada tag barunya dan pengguna tersebut dapat melakukan penghapusan objek, review atau edit objek metadata seperti (nama, tipe, gambar, atau kapan terakhir tag dibaca oleh reader). Tools yang kedua yaitu *place manager* yang digunakan untuk memunculkan setiap RFID antenna dengan label di Google Maps. Aplikasi yang ketiga yaitu kontrol privasi, memungkinkan pengguna untuk memberikan pengaturan hak akses dalam mengumpulkan data RFID melalui aplikasi berbasis web. Ide utama aplikasi ini adalah bahwa akses pengguna dibatasi pada peristiwa yang terjadi hanya ketika dan di mana mereka hadir secara fisik. Dengan cara ini, data RFID pribadi mereka dapat berfungsi sebagai catatan terperinci tentang peristiwa yang mungkin telah mereka amati secara langsung sepanjang hari.

Didalam jurnal ini juga dikembangkan beberapa aplikasi RFID berbasis web lain yang berkaitan dengan penerapan *Internet of Things* yaitu:

1. A Search Engine for Things yaitu aplikasi RFID berbasis web sederhana yang memungkinkan pengguna melihat lokasi yang terakhir direkam atau mencari lokasi objek tertentu dan aplikasi akan memberikan notifikasi.
2. Social Application yang bernama Rfidder menggunakan aktifitas pengguna dan tempat untuk memberikan informasi secara *real-time* pada pembaharuan di sosial media.
3. Personal Trends yaitu aplikasi pencatatan historis tentang objek dan data *events* yang memungkinkan pengguna mempelajari tren dalam aktivitas mereka dari waktu ke waktu. Ini bisa sangat berguna untuk aplikasi yang mendukung kegiatan jangka panjang seperti proyek bisnis dan kolaborasi.
4. Event-Based Desktop Search yaitu aplikasi pencatatan peristiwa yang dikumpulkan oleh aplikasi seperti *Digital Diary*.

2.2.2 Kontrol Kehadiran

Dalam penelitian yang dilakukan oleh Nurbek Saparkhojayev dan Selim Guvercin di Universitas Nasional Eurasian, Kazakhstan yang berjudul *Attendance Control System based on RFID-technology* (Saparkhojayev & Guvercin, 2012) menyatakan bahwa pengecekan kehadiran siswa merupakan suatu isu permasalahan yang penting. Di beberapa universitas kehadiran merupakan suatu komponen yang penting ketika dosen akan memberikan nilai akhir kepada mahasiswa selama mahasiswa tersebut kuliah dalam satu semester. Beberapa universitas masih ada yang mencatat kehadiran mahasiswanya menggunakan kertas dan melakukan *input* data ke sistem secara manual. Dosen akan melakukan absensi dengan memanggil mahasiswa satu per satu dan hal ini akan memakan waktu sekitar 10 menit dari jam pelajaran. Terkadang jika ada mahasiswa yang tidak hadir, mereka membeberitahukan kepada teman mereka yang hadir didalam kelas bahwa mereka tidak bisa mengikuti kelas. Berdasarkan permasalahan yang dipaparkan diatas, penulis jurnal tersebut membuat penelitian untuk membuat sistem yang akan memudahkan dalam melakukan pengecekan kehadiran mahasiswa secara otomatis

berbasis teknologi RFID. RFID tag atau kartu memiliki ID yang unik. RFID-reader akan membaca setiap kartu mahasiswa ketika memasuki ruang kelas dan mengirim data tersebut ke server. Hal ini tentunya akan membuat waktu belajar di kelas lebih maksimal.

Dibandingkan dengan teknologi otomasi identifikasi lainnya seperti *optical barcode* dan *irish pattern*, RFID memiliki beberapa kelebihan yaitu otentikasi yang lebih cepat, hemat daya, lebih murah, mudah dibawa, lebih stabil dan tentunya mudah untuk dikembangkan. RFID tag yang digunakan dalam penelitian ini yaitu MIFARE MF11CS50 merupakan *contactless smart card* berdasarkan ISO/IEC 14443 type A yang biasa digunakan untuk ururan tiket transportasi. RFID-tag yang dipilih dalam penelitian ini adalah tag yang dapat bekerja pada frekuensi LF, HF, dan UHF karena disesuaikan dengan frekuensi yang bekerja di negara tersebut yang berarti menggunakan RFID-tag passive. Energi dan datanya dikirimkan via antenna. EHUOYAN's YHU638 digunakan sebagai RFID-reader karena harganya yang murah dan mudah digunakan. Penelitian ini bertujuan untuk membuat sebuah sistem dimana semua perangkat saling terhubung yang akan memudahkan dalam melakukan *monitoring* dan sistem ini dibangun berbasis desktop. Dosen yang telah hadir dikelas melakukan login ke sistem melalui komputer di kelas. Dalam implementasinya, sistem ini membutuhkan komputer disetiap kelas yang terhubung dengan RFID-reader yang dapat membaca kartu pengguna dan juga tersedianya *web camera* untuk mengambil foto pengguna. Hal ini bertujuan untuk mencegah siswa tersebut menitipkan kartunya kepada temannya apabila ia tidak masuk kelas. Pada akhir sesi pembelajaran dosen melakukan submit data ke dalam basis data.

2.2.3 Pengamanan Ruang Menggunakan RFID

Penelitian yang dilakukan oleh Gyanendra Kumar Verma yang berjudul *A Digital Security with Door Lock System Using RFID Technology* (Verma & Tripathi, 2010) 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*.

Nantinya sistem ini akan di manajemen secara terpusat terkait pengoperasian dan transaksi yang terjadi pada RFID. RFID merupakan suatu sistem yang komprehensif 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. Hal ini bisa menjadi solusi dari suatu permasalahan saat ini tentang mengamankan sebuah ruangan yang sangat privasi. Secara sederhana sistem ini memerlukan beberapa perangkat keras dan lunak yang perlu dikembangkan. Perangkat keras yang dibutuhkan dalam sistem ini yaitu RFID reader, tags, koneksi USB, koneksi kabel dan komputer serta basisdata.

Secara umum rangkaian tahapan proses otentikasi dan validasi dalam sistem ini akan dijabarkan sebagai berikut:

1. RFID menerima informasi dari tag ketika didekatkan ke reader.
2. Setelah menerima informasi dari tag, reader mengirimkan data ke basisdata server untuk melakukan konfirmasi.
3. Selanjutnya server akan melakukan pencarian informasi yang diterimanya dari reader didalam basis data
4. RFID-reader akan melakukan komputasi untuk melakukan pencatatan aktivitas (log) misalnya *timestamp* setelah menerima balasan dari server.

5. Setelah tag diverifikasi, sistem akan memproses sinyal melalui port yang mengontrol pembuka dan pengunci pintu.

Cara kerja sistem ini yaitu RFID-reader terkoneksi dengan USB port agar dapat berkomunikasi antara sistem dan RFID-reader. Sistem akan menyimpan semua informasi terkait pengguna seperti nama, id, kategori, *check-in-time*, *check-out-time*, tanggal dan lain sebagainya. Ketika ada seorang pengguna yang datang mendekati sebuah pintu, maka dia akan menempelkan kartu ke RFID-reader. Jika pengguna tersebut terdaftar dalam basisdata maka pengguna tersebut dapat mengakses pintu dan interval waktu penggunaan ruangan akan dihitung oleh sistem.

2.2.4 Access Control System

Dalam penelitian yang berjudul *Development of an RFID Based Access Control System in the Context of Bangladesh* (Shafin et al., 2015) 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 *manage* 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 yang 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 validasi 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* (Bajer, 2017) 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*. Perbandingan penerapan RFID dari penelitian terkait ditunjukkan pada Tabel 2.3 berikut:

Tabel 2.3 Tabel Perbandingan Penerapan RFID

No	Nama Penulis	Judul Tesis	Tujuan	Solusi
1.	Welbourne et al., 2009	<i>Building the Internet of Things Using RFID</i>	Penerapan Internet of Things (IoT) untuk keperluan manajerial, pengaturan privasi dan kontrol data pengguna	Mengkombinasikan RFID dengan aplikasi berbasis web atau internet sehingga tercipta sebuah inovasi penerapan RFID berbasis IoT.
2.	Saparkhojayev & Guvercin, 2012	<i>Attendance Control System based on RFID-technology</i>	Pencatatan absensi (menggantikan kertas) dan <i>input data</i> ke sistem tidak dilakukan lagi secara manual	Penerapan RFID sebagai alat untuk melakukan absensi otomatis dan <i>input data</i> secara langsung ke sistem.
3.	Verma & Tripathi, 2010	<i>A Digital Security with Door Lock System Using RFID Technology</i>	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 <i>backend</i> aplikasi yang mampu mengintegrasikan antara RFID-reader dengan basis data akun pengguna.

4.	Shafin et al., 2015	<i>Development of an RFID Based Access Control System in the Context of Bangladesh</i>	Mengamankan ruang dengan membuat sistem kontrol akses pengguna yang dapat memberi izin pengguna untuk mengakses sebuah ruangan misal berapa lama pengguna dapat	Menggunakan teknologi RFID untuk melakukan otentikasi pengguna ruangan yang diintegrasikan dengan basisdata akun pengguna melalui aplikasi <i>backend</i> yang dikembangkan.
	Bajer, 2017	<i>Extension of Genway ECK-03a door control system to work as a part of Elastic based smart building system</i>	mengakses ruangan tersebut, mencatat aktivitas pengguna dan memvisualisasikan aktivitas pengguna tersebut (log)	Mengkombinasikan teknologi RFID dengan tools <i>Elastic Stack</i> dengan mengembangkan aplikasi <i>backend</i>

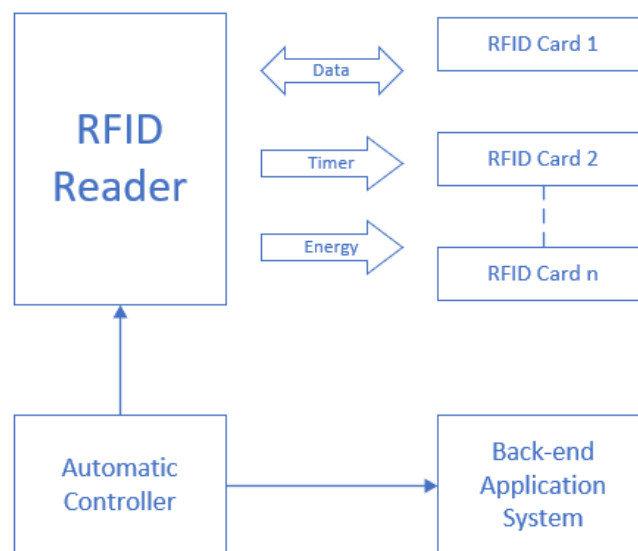
2.3 Tipikal Arsitektur Sistem RFID

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 komprehensif 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 (Verma & Tripathi, 2010).

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 (Verma & Tripathi, 2010). Secara umum tipikal sistem arsitektur RFID digambarkan seperti Gambar 2.4 berikut:



Gambar 2.4 Tipikal Sistem RFID

Sumber: (Verma & Tripathi, 2010)

2.4 Kesimpulan dari Penelitian Sebelumnya

Sesuai permasalahan yang telah dipaparkan dari penelitian sebelumnya, setiap institusi, instansi atau universitas menggunakan teknologi RFID untuk keperluan yang berbeda-beda. Setiap instansi atau institusi mengembangkan aplikasi dengan menerapkan teknologi RFID sesuai dengan kebutuhan atau masalah yang sedang dihadapi oleh instansi tersebut. Misalnya suatu universitas memiliki masalah terhadap lambatnya pencatatan kehadiran mahasiswa dikarenakan prosedur yang masih dilakukan secara manual seperti jurnal yang telah dibahas sebelumnya, maka universitas tersebut mengembangkan sebuah aplikasi yang dapat melakukan pencatatan absensi secara otomatis. Teknologi RFID dipilih dikarenakan di setiap RFID-tag terdapat ID unik yang dapat digunakan untuk melakukan identifikasi dan validasi pengguna dengan mencocokkannya terhadap akun yang telah terdaftar di dalam basis data. Di sisi lain Teknologi RFID juga dimanfaatkan untuk bidang keamanan atau *security* contohnya pengaksesan ruang. Dengan menggunakan teknologi RFID tentunya hal ini akan memudahkan suatu instansi untuk melakukan validasi dan otentikasi terhadap pengguna yang ingin mengakses sebuah ruangan dengan memanfaatkan ID unik dari RFID-tag tersebut. Contoh luas penerapan RFID di bidang lainnya yaitu kombinasi antara teknologi RFID dengan *Internet of Things* karena pada saat ini teknologi jaringan wireless sedang berkembang pesat. Salah satu penerapannya adalah dapat mengetahui aktivitas dan lokasi pengguna secara *real-time*. Hal ini menunjukkan bahwa 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 seperti RFID-reader, RFID-tag, dan *backend* aplikasi sehingga RFID dapat digunakan untuk menyelesaikan permasalahan sesuai dengan kebutuhan instansi terkait.

Pembahasan mengenai permasalahan dan solusi yang digunakan menggunakan teknologi RFID dapat digunakan sebagai acuan dalam penerapan untuk pengamanan ruangan yang ada di Universitas Islam Indonesia (UII). Dengan banyaknya ruangan, seperti laboratorium atau ruang penting lainnya dan banyaknya pengguna atau *user* di UII 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 lingkungan UII.