Perbandingan Teknologi *Wireless* untuk Sistem Absensi pada *Smart University*

Muhammad Syarifudin[1], Budi Rahadjo[2]
Institut Teknologi Bandung
Jalan Ganesha No 10, 022-2500935
e-mail: muhammad.el.syarifudin@gmail.com[1], rahard@gmail.com[2]

Abstrak – *Salah satu metode untuk melihat kinerja pegawai maupun kesadaran sebagai mahasiswa yaitu dengan adanya sistem absensi. Saat ini, teknologi wireless sedang berkembang pesat. Berbagai instansi dan industri banyak menggunakan infrastruktur jaringan berupa wireless serta aplikasi yang menggunakan teknologi wireless dalam kegiatan sehari-hari. Wireless sangat diperlukan untuk pengguna dengan mobilitas tinggi. Untuk implementasinya, standar jaringan nirkabel sudah dibuat seperti IEEE 802.15.1 Bluetooth, IEEE 802.11 WiFi dan IEEE 802.15.4 ZigBee. Artikel ini memberikan informasi rinci, analisis, dan pembahasan state-of-the-art tentang modul komunikasi wireless seperti Bluetooth, ZigBee, dan NFC dalam aplikasi internet of things untuk membangun smart university. Tulisan ini juga membahas perbandingan keseluruhan modul dan karakteristik seperti standar, bandwidth, daya tahan baterai, data rate, dan jangkauan transmisi maksimum.*

Kata kunci*: absensi, wireless, internet of things, smart university.*

1. Pendahuluan

Smart office, *smart hospital*, dan *smart building* merupakan implementasi dari perkembangan *internet of things* [1]. *Smart University* juga merupakan hasil perkembangan *internet of things* yang dapat mengintegrasikan devais-devais di suatu institusi atau universitas tertentu. Penerapan teknologi yang tepat sangat diperlukan untuk implementasi, sehingga diperlukan bahasan khusus tentang teknologi yang sudah ada dan berbagai macam alternatif untuk menerapkannya ke dalam aplikasi *internet of things* yang diinginkan.

Satu dekade ini, teknologi wireless berkembang dengan pesat. Teknologi ini memungkinkan untuk mengirimkan data secara efisien dan memiliki jangkauan luas. Teknologi wireless ini sangat mendukung banyak aplikasi dalam implementasinya. Teknologi ini juga dapat di kembangkan dengan menambahkan berbagai macam devais seperti *sensor*, *actuator*, dan *smartphone* [2].

Penerapan teknologi untuk aplikasi *internet of things* bergantung pada infrastruktur yang ada di suatu wilayah, biaya yang diperlukan untuk implementasi, dan tingkat efektifitas dari teknologi yang diterapkan. Aplikasi teknologi wireless semakin banyak digunakan karena teknologi ini membuat komunikasi yang handal untuk diimplementasikan di berbagai bidang [2]. Keuntungan yang diperoleh ketika menggunakan teknologi wireless adalah mobilitas yang tinggi dan dapat terkoneksi tanpa menggunakan kabel.

Berdasarkan uraian di atas, penerapan teknologi yang mudah dan murah sangat diperlukan untuk berbagai aplikasi *internet of things*. Dengan perkembangan teknologi wireless ini diharapkan dapat meningkatkan mobilitas dan efektifitas penggunaan teknologi. Selain itu, keamanan yang ditawarkan untuk setiap teknologi akan sangat diperhatikan agar tidak merugikan banyak orang.

Implementasi *internet of things* sangat beragam. Konsepnya yaitu dapat menggabungkan berbagai devais yang terkoneksi dengan menggunakan internet. Beragamnya devais dan teknologi yang terkait *internet of things* membuat desainer harus mempelajari banyak hal untuk menentukan teknologi yang sesuai dengan kriteria tertentu.

Makalah ini akan membahas informasi rinci, analisis, dan state-of-the-art tentang modul komunikasi wireless seperti Bluetooth, ZigBee, NFC, dan GSM dalam aplikasi *internet of things* untuk membangun *smart university*. Selain itu, makalah ini juga membahas perbandingan keseluruhan modul dan karakteristik seperti standar, bandwidth, daya tahan baterai, data rate, dan jangkauan transmisi maksimum.

2. Metode Penelitian

Pada penelitian ini dilakukan beberapa metode untuk mencapai tujuan dibangunnya *smart university*. Metode tersebut diharapkan dapat memberikan gambaran teknologi yang akan digunakan untuk desain dan implementasi sistem absensi menggunakan teknologi wireless. Metode yang digunakan adalah sebagai berikut.

2.1. Studi Pustaka

Metode ini dilakukan dengan mencari dan mengumpulkan informasi melalui internet, datasheet, forum online, product manual, dan laporan yang berkaitan langsung dengan topik. Hal utama yang menjadi fokus makalah ini adalah studi pustaka tentang teknologi wireless dan devais yang mungkin untuk digunakan dan aplikasinya.

2.2. Komparatif

Metode ini dilakukan dengan mengumpulkan informasi terkait dengan teknologi wireless dan devaisnya. Kemudian, setiap devais dibandingkan dengan karakteristik tertentu untuk melihat spesifikasi yang digunakan.

2.3. Survey

Metode ini dilakukan untuk mengumpulkan informasi pada institusi atau universitas tentang data pegawai dan data mahasiswa sehingga diperoleh spesifikasi teknologi wireless yang diperlukan untuk membangun sistem terintegrasi pada *smart university*.

2.4. Analisis

Analisis dilakukan dengan menganalisa perbandingan setiap teknologi yang telah diperoleh pada metode sebelumnya dan menganalisa devais yang memungkinkan untuk diimplementasikan ke dalam aplikasi *internet of things* untuk membangun *smart university* serta sistem keamanan yang digunakan. Selain itu, analisis akan membahas tentang kelebihan dan kekurangan setiap devais pada kasus-kasus tertentu. Hasil analisis ini akan dijadikan pertimbangan untuk menentukan teknologi yang sesuai untuk digunakan pada sistem absesnsi.

2.5. Pengembangan Metode

Setelah mengetahui berdasarkan survey dan analisis yang telah dilakukan, maka dilakukan kajian untuk meningkatkan keamanan pada sistem absensi yang akan diimplementasikan untuk aplikasi *smart university*. Sistem absensi ini akan terintegrasi dengan internet sehingga tidak dapat dimanipulasikan baik oleh pegawai atau mahasiswa.

ISBN: 978-602-60581-0-2

3. Hasil dan Analisis

Berdasarkan metode penelitian yang telah dilakukan, hasil dan analisis tentang sistem absensi menggunakan teknologi wireless adalah sebagai berikut.

3.1. Hasil

Hasil yang diberikan merupakan tinjauan dari sisi teknologi yang memungkinkan untuk menerapkan sistem absensi dengan mendeskripsikan semua teknologi wireless yang banyak digunakan saat ini, yaitu Bluetooth, ZigBee, dan NFC. Berikut penjelasan tentang devais sistem komunikasi menggunakan teknologi wireless untuk diimplementasikan ke sistem absensi yang berbasis aplikasi *internet of things.*

3.1.1. Bluetooth

Bluetooth sering digunakan pada sebuah organisasi atau individu untuk menyediakan wireless personal area network (WPAN). Hal tersebut dikarenakan gelombang radio frequency (RF) pada bluetooth dapat dengan mudah menembus penghalang dan propagasi gelombangnya dapat dilakukan tanpa direct line-of-sight (LoS). WPAN merupakan jaringan wireless dengan jarak pendek yang mendukung devais *portable* dan *mobile computing*. Teknologi Bluetooth dikembangkan untuk menggantikan kabel menggunakan WPAN. Bluetooth dapat digunakan secara global karena bebas lisensi dan dapat digunakan untuk *Industrial, Scientific, and Medical* (ISM) band pada 2,4 GHz [3].

Bluetooth bekerja dengan baik di lingkungan yang banyak sinyal noise. Bluetooth beroperasi berdasarkan fitur Adaptive Frequency Hopping (AFH) dan Forward Error Correction (FEC) sehingga dapat menyediakan kemampuan jaringan nirkabel jarak pendek yang universal [2]. Bluetooth yang beroperasi pada frekuensi band 2,4 GHz menggunakan Frequency-Hopping Spread Spectrum (FHSS) [3] sehingga dapat mentransmisikan sinyal suara sebagai data. Bluetooth menyediakan bandwidth yang dapat melayani pertukaran data antar devais sampai 1 Mbps untuk versi 2.0 dan sebelumnya serta sampai 3 Mbps untuk versi 2.1 dan setelahnya. Jangkauan teknologi Bluetooth dapat menjapai 10 m antar devais untuk pertukaran data [3].

Teknologi Bluetooth terauthentikasi dengan mengirimkan *acknowledgement* dari *receiver* ke *transmitter* sebelum membuat koneksi antar devais. Bluetooth memiliki keterbatasan hanya delapan devais yang dapat berkomunikasi dalam satu jaringan dan selalu meminta konfirmasi setiap menerima data setiap waktu serta dibatasi paket size yang dikirimkan [2]. Namun, tingkat keamanan pada Bluetooth masih sangat rentan terhadap serangan seperti *eavesdropping*, *man in the middle* (*MITM)* dan *jamming attack*. Bluetooth menggunakan salah satu dari teknologi pairing yaitu *legacy pairing* atau *secure and simple pairing* (SSP) [3].

Metode *legacy pairing* membutuhkan masukan dari setiap devais berupa Personal Identity Number (PIN) untuk melakukan *pairing*. *Pairing* akan sukses ketika kedua devais memasukkan PIN yang sama. Secara default, Bluetooth diprogram dengan 4 digit PIN sehingga dapat dipastikan adanya keterbatasan kunci untuk keamanannya. Oleh karena itu, selama pairing sangat rentan terhadap serangan dari *attacker* untuk mendapatkan PIN dari devais [3].

Sedangkan SSP menggunakan bentuk kriptografi kunci publik dan beberapa jenis keamanan yang dapat membantu melindungi terhadap serangan MITM sehingga lebih aman dari serangan attacker ketika melakukan *pairing* [3]. SSP dianggap sederhana karena dalam kebanyakan kasus, tidak memerlukan *user* untuk menghasilkan kode akses. Untuk penggunaan yang tidak memerlukan perlindungan MITM, interaksi antar *user* dapat dihilangkan.

Kelebihan Bluetooth adalah sebagai berikut [4].

1. Bluetooth tidak memerlukan kabel ataupun kawat.
2. Bluetooth dapat menembus dinding, kotak, dan berbagai rintangan lain walaupun jarak transmisinya hanya sekitar 30 kaki atau 10 meter.
3. Berdaya rendah dan hardware relatif kecil.
4. Bluetooth dapat mensinkronisasi basis data dari telepon genggam ke komputer.
5. Dapat digunakan sebagai perantara modem.

ISBN: 978-602-60581-0-2

Kekurangan Bluetooth adalah sebagai berikut [4].

1. Sistem ini menggunakan frekuensi yang sama dengan gelombang LAN standar sehingga memungkinan terjadinya interferensi dengan teknologi lain yang menggunakan ISM band.
2. Apabila dalam suatu ruangan terlalu banyak koneksi Bluetooth yang digunakan, akan menyulitkan pengguna untuk menemukan penerima yang diharapkan.
3. Banyak mekanisme keamanan Bluetooth yang harus diperhatikan untuk mencegah kegagalan pengiriman atau penerimaan informasi.
4. Di Indonesia, sudah banyak beredar virus yang disebarkan melalui bluetooth dari telepon genggam.
5. Kecepatan dalam transfer data tidak tetap, tergantung dari perangkat yang dipakai untuk mengirim dan yang menerima data maupun informasi.

Gambar 1. Jaringan Bluetooth

3.1.2. ZigBee

ZigBee merupakan teknologi komunikasi wireless yang digunakan untuk WPAN. Teknologi ini telah distandarkan pada tahun 2003 yaitu standar IEEE 802.15.4. ZigBee beroperasi pada ISM band, yaitu 2,4 GHz [1]. Komunikasi ZigBee secara khusus dibangun untuk kontrol dan sensor jaringan pada standar IEEE 802.15.4 untuk WPAN. Komunikasi standar ini mendefinisikan *Physical* dan *Media Access Control* (MAC) *layer* untuk menangani banyaknya devais pada tingkat data yang rendah. ZigBee juga dapat beroperasi pada frekuensi 868 MHz, 902-928MHz dan 2,4 GHz. Data rate yang digunakan adalah 250 Kbps [5]. Data rate tersebut merupakan yang paling cocok untuk transmisi dua arah data antara sensor dan pengendali secara periodik. Karena konsumsi daya yang rendah, perangkat ZigBee dapat mengirimkan data dalam jangkauan transmisi antara 10 meter sampai 100 meter [5].

Topologi jaringain yang digunakan pada komunikasi ZigBee adalah *mesh* dan *star* untuk antarmuka antara satu sama lain [5]. ZigBee menyediakan topologi jaringan untuk komunikasi antar devais dan memberikan fitur komunikasi tambahan seperti authentikasi, enkripsi dan asosiasi dengan layanan aplikasi di layer yang lebih tinggi. ZigBee memiliki banyak keunggulan yang ditawarkan seperti biayanya murah untuk *deployment* atau *redeployment*, jaringan *mesh* pada ZigBee dapat mencakup area yang cukup luas, dan beroperasi menggunakan baterai [2].

ZigBee mendukung konfigurasi jaringan yang berbeda untuk komunikasi *master to master* atau *master to slave*. Selain itu, dapat dioperasikan dalam berbagai mode sehingga dapat menghemat daya baterai yang digunakan. Jaringan ZigBee dapat diperpanjang dengan menggunakan router dan memungkinkan banyak node untuk menghubungkan satu sama lain untuk membangun jaringan area yang lebih luas.

Terdapat dua tipe *node* pada jaringan ZigBee sehingga operasi dari sebuah *node* ZigBee tergantung pada apakah itu adalah full-function device (FFD) atau reduce-function device (RFD). FFD melakukan semua tugas yang didefinisikan oleh standar ZigBee sedangkan fungsi

ISBN: 978-602-60581-0-2

yang dilakukan oleh RFD terbatas. Sebuah FFD dapat membentuk topologi jaringan (seperti *star*, t*ree*, atau *mesh*) sementara RFD hanya dapat terhubung ke sebuah FFD [6].

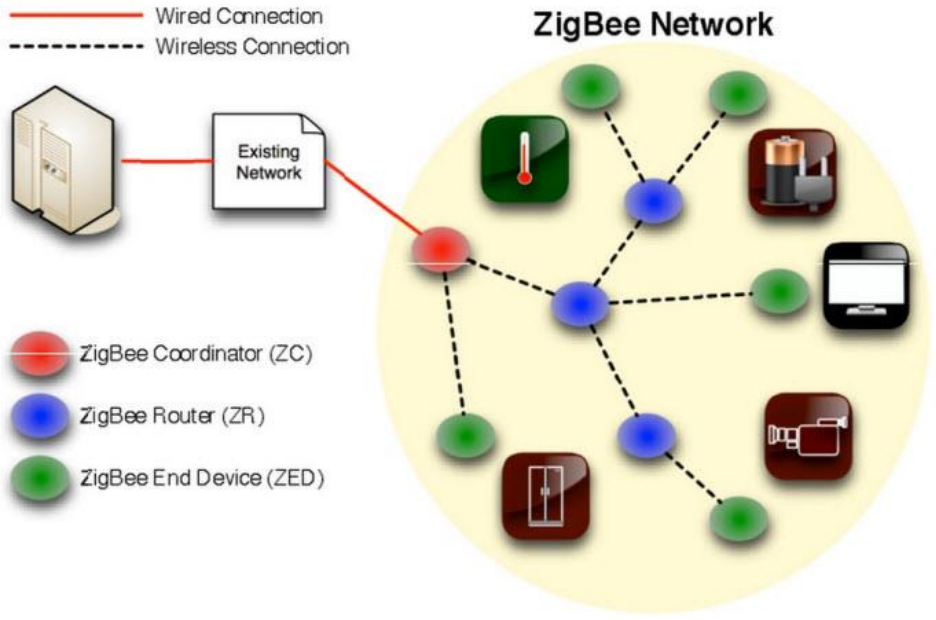
Berdasarkan fungsi tersebut, perangkat ZigBee diklasifikasikan sebagai *Coordinator*, *Router* dan *End Devices*. *ZigBee Coordinator (ZC)* merupakan sebuah FFD dan sebuah jaringan hanya terdiri dari satu buah *ZC*. *ZigBee Router (ZR)* juga merupakan sebuah FFD dan dapat juga tidak ada dalam jaringan. Sebuah jaringan dapat terdiri dari satu atau lebih *ZR* tergantung pada ukuran dan topology jaringan. *ZigBee End Devices (ZED)* merupakan RFD dan biasanya terdapat pada ujung-ujung suatu jaringan. Tugas utamanya yaitu mengirimkan dan menerima paket data. Namun, devais lain tidak dapat terkoneksi ke jaringan melalui ZED.

Dari segi keamanan, ZigBee menyediakan otentikasi, integritas, dan privasi dalam jaringan ZigBee. Keamanan yang disediakan menggunakan enkripsi *counter mode* dan *cipher block chaining message authentication code* (CCM) pada tingkat yang berbeda dengan algoritma Advanced Encryption Standard (AES) 128 bit [7].

Untuk semua tingkat keamanan, ZigBee menggunakan kunci simetris dan mengaplikasikan kriptografi serta integritas untuk *network* dan *application layer*. ZigBee menggunakan 3 jenis kunci untuk keamanan, yaitu: link, network dan master keys. Pada implementasinya, tingkat keamanan jaringan ZigBee merupakan tanggung jawab dari developer yang menerapkan teknologi menggunakan ZigBee [6].

Standar keamanan yang digunakan dalam transceiver ZigBee saat berkomunikasi dengan node lainnya yaitu menggunakan algoritma Advanced Encryption Standard (AES). Panjang kuncinya adalah 128 bit. Sebuah metode enkripsi yang unik diperlukan karena pada faktanya sebagian besar transceiver ZigBee memiliki desain hardware tertentu. Algoritma AES juga digunakan untuk *Data Integrity* [5]. Hal ini dilakukan dengan menambahkan *Message Authentication Code (MAC)* ke pesan. Ukuran MAC dapat bervariasi dari 32 menjadi 128 bit, namun sebagian besar dibuat menggunakan algoritma AES 128 bit [8]. Keamanan data dilakukan dengan mengenkripsi *data payload field* dengan kunci 128 bit.

Zigbee mempunyai beberapa kelebihan antara lain fleksibel dalam pengiriman data, biaya yang relatif murah serta rentang jaringan yang kurang dari 100 meter, yang memudahkan dalam instalasi jaringan. Kekurangnnya adalah keamanan pada zigbee ini masih rentan terhadap serangan dikarenakan standar dari spesifikasi IEEE 802.15.4 yang masih cacat. Hal ini terbukti dari beberapa penelitian yang dilakukan terhadap aplikasi yang berjalan para zigbee tersebut. Oleh karena itu, parancang aplikasi zigbee di harapkan dapat memperbaiki kekurangan yang ada pada sistem kemanan zigbee tersebut [9].



Gambar 2. Jaringan ZigBee

ISBN: 978-602-60581-0-2

3.1.3. NFC

Near Field Communication (NFC) adalah bentuk *short-range* dari frekuensi radio yang digunakan pada teknologi komunikasi nirkabel berdaya rendah untuk perangkat elektronik. NFC memungkinkan berkomunikasi antar devais dengan bersentuhan lunak atau mendekatkannya pada jarak yang sangat dekat. Cara untuk berkomunikasi antar devais tersebut dapat dikatakan sebagai '*tap-in*' atau '*to tap and go'*. Protokol komunikasi NFC biasanya dapat terjadi antara dua perangkat aktif seperti *smartphone* dan laptop atau bahkan antara perangkat NFC dan pasif (unpowered) *'tag'* [10].

Perangkat pertama biasanya disebut inisiator yang menggunakan induksi magnetik untuk menciptakan *field* gelombang radio sehingga target (perangkat kedua) dapat mendeteksi, mengakses, dan memungkinkan pertukaran sejumlah data kecil yang akan ditransfer secara nirkabel melalui jarak yang relatif singkat. Dalam kasus NFC ini, jarak secara umum harus kurang dari 4 inci [10].

Saat ini, NFC dapat digunakan pada banyak aplikasi dan fokus utamanya di bidang identifikasi dan otentikasi, sistem ticketing di transportasi umum, serta pembayaran elektronik contactless Elektronik Point of Sales (EPOS) terminal di pusat perbelanjaan [10]. NFC adalah pengembangan dari teknologi Radio Frequency Identification (RFID) yang digunakan ke dalam perangkat handphone untuk memudahkan transaksi. NFC beroperasi pada frekuensi 13.65 MHz dengan rata – rata kecepatan transfer 106 Kbps sampai 848 Kbps [11].

Cara kerja NFC sendiri mirip dengan Bluetooth dan Wi-Fi, yaitu melakukan koneksi Wireless berbasis frekuensi radio [12]. Perbedaannya sebagai berikut:

1. Koneksi Bluetooth/WiFi menggunakan setting teknis tertentu, NFC hanya perlu melakukan Tap (mendekatkan *Smartphone* pada terminal NFC).
2. Bluetooth & WiFi menggunakan frekuensi 2.4 – 2.5 GHz, sedangkah NFC menggunakan frekuensi rendah 13.56 MHz.
3. Jarak transfer Bluetooth ~ 3m, WiFi ~ 100m, sedangkan NFC tidak lebih dari 20 cm.
4. NFC hanya mentransfer data kapasitas rendah (satuan kilobyte), karena hanya untuk melakukan otorisasi, informasi kecil, transaksi & pembayaran.
5. Waktu setup koneksi NFC hanya < 0,1 detik, sedangkan Bluetooth/WiFi bisa lebih dari 6 detik.

NFC memerlukan dua perangkat untuk berkomunikasi, yaitu NFC Reader dan NFC Tags. NFC Reader adalah *Smartphone/*Tablet pengguna dengan fitur NFC. NFC Tags sendiri merupakan terminal kecil berisi sebuah Chip (IC) NFC dengan antena radio terintegrasi. NFC Tag dapat menyimpan berbagai informasi yang ditentukan oleh penggunanya, misalnya informasi diskon, peta, harga atau tiket. Jadi saat melakukan pembayaran *Smartphone* dan NFC Tag akan didekatkan, lalu terjadi transaksi otomatis [12].

Pada prinsipnya, kedua perangkat NFC menggunakan medan elektromagnetik untuk melakukan transfer data. Saat kita mendekatkan *Smartphone* ke Terminal NFC, NFC Reader akan mengaktifkan signal didalam NFC Tag. Lalu kedua perangkat ini langsung berkomunikasi, dimana NFC Reader mengambil informasi didalam NFC Tag. NFC Reader mengirimkan informasi itu ke server [12].

Kelebihan NFC sebagai berikut:

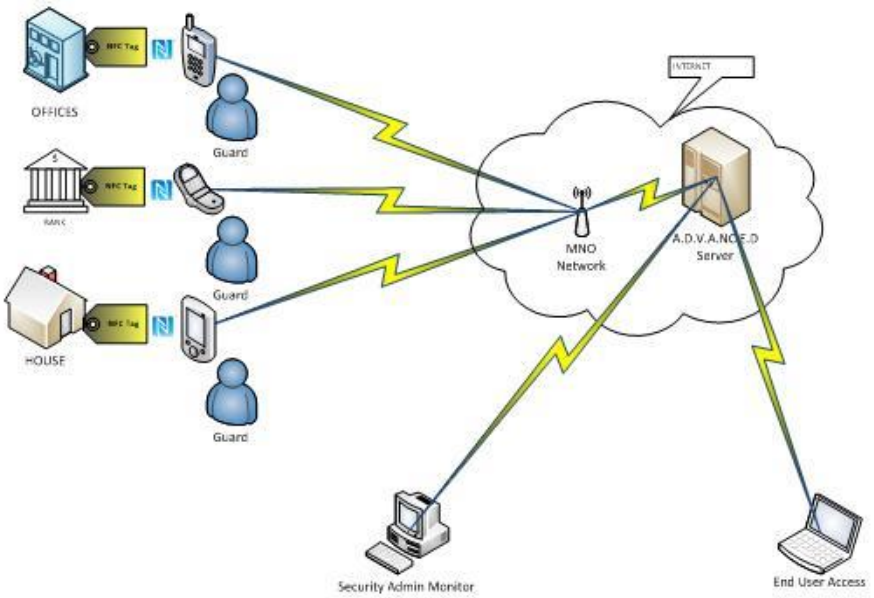
1. Tag NFC dan kartu tidak mengkonsumsi daya [10].
2. Sedikit kemungkinan untuk terjadi gangguan saat koneksi karena menggunakan system RFID [10].
3. Mempermudah dalam melakukan transaksi karena NFC telah terintegrasi dengan *smartphone* [11].
4. Memungkin interaksi dua arah antar perangkat elektronik yang lebih aman dan simple [13].
5. Kecepatan konektivitasnya lebih cepat [13].
6. Melakukan transaksi secara contactless, mengakses konten digital dan melakukan koneksi dengan perangkat elektronik hanya dengan satu sentuhan. [13].

ISBN: 978-602-60581-0-2

7. Keunikan dari NFC ini terletak pada kemampuannya untuk mengubah mode operasinya menjadi reader/writer, peer to peer, atau card emulation. Mode operasi yang berbeda tersebut berdasar pada ISO/EIC 18092 dan ISO/EIC 14443 contacless smart card standard [13].

Kelemahan NFC sebagai berikut [13].

1. Harga perangkat NFC yang tidak murah, seperti harga smartphone yang masih cukup mahal untuk saat ini.
2. Device yang mendukung teknologi ini masih sangat sedikit.
3. Jangkauan transmisi yang jauh lebih pendek daripada Bluetooth.
4. Kecepatan transfer data NFC sedikit lebih lambat.



Gambar 3. Diagram Jaringan Menggunakan NFC

Gambar 4. Contoh Aplikasi NFC

ISBN: 978-602-60581-0-2

3.2. Analisis

Analisis pada tulisan ini didasarkan pada metode penelitian yang dilakukan. Bahasan pada analisis ini dibatasi tentang perbandingan performansi devais dan spesifikasi sistem absensi yang memungkinkan untuk diimplementasikan pada sebuah universitas atau institusi tertentu.

3.2.1 Perbandingan Performansi Devais

Berikut adalah tabel perbandingan lengkap spesifikasi dari teknologi wireless yang memungkinkan untuk digunakan pada sistem absensi dalam membangun *smart university*.

Table 1. Tabel Performansi untuk Devais Komunikasi

	NFC	Bluetooth	ZigBee
Standar Internasional	ISO 14443	IEEE 802.15.1	IEEE 802.15.4
Set-up time	<0,1 ms	6 sec	30ms
Range	Up to 10 cm	Up to 30 m	10-100m
Operating Frequency	13,56 MHz	2,4 GHz	868 MHz (eropa)
Maximum Data Rate	0,42 Mbps	3 dan 22 Mbps	20, 40, dan 250 kbps
Complexity	Low	High	Low
Usability	Human centric Easy intuitive, fast	Data centric medium	Wireless mesh network
Selectivity	High, given, security	Who are you?	Secure communication
Use cases	Pay, get access, share, initiate service, easy set up	Network for data exchange, headset	Industrial control, home control, building automation, smoke and intruder warning
Consumer experience	Touch, wave, simply connect	Configuration needed	Device can join an existing network
Cost	Low	Low	Low
Power Consumption	∞	Hours/day	Very low months/years
Directional Communication	Two way	Two way	Two way

3.2.2. Spesifikasi Alat untuk Sistem Absensi

Implementasi sistem absensi pada suatu institusi atau universitas tidak hanya mahasiswa, tetapi pegawai dan dosen pun terlibat sehingga sistem absensi ini diharapkan dapat digunakan dimana saja dalam satu cakupan wilayah tertentu. Sistem absensi ini diharapkan tidak memerlukan waktu yang lama dan dari lebih *secure*. Selain itu, alat yang digunakan harus hemat energi dan relatif murah. Sistem ini juga dapat dengan mudah dikembangkan dan diintegrasikan dengan sistem lain.

Spesifikasi alat yang cocok untuk membangun *smart university* pada sistem absensi adalah ZigBee. ZigBee memiliki banyak kelebihan yang ditawarkan seperti biaya yang diperlukan rendah, mudah untuk dikembangkan, dan menyediakan topology jaringan yang memungkinkan banyak devais yang terhubung. ZigBee juga menggunakan baterai yang dapat bertahan lama.

ISBN: 978-602-60581-0-2

Keunggulan utama ZigBee pada sistem absensi untuk smart university adalah jangkauan komunikasi menggunakan ZigBee cukup ideal untuk suatu institusi atau universitas.

4. Kesimpulan

Sistem absensi dalam membangun *smart university* dapat diimplementasikan menggunakan teknologi *wireless*. Terdapat beberapa teknologi yang memungkinkan, yaitu NFC, ZigBee, dan Bluetooth. Masing-masing teknologi memiliki banyak keunggulan dan kekurangan. Berdasarkan metode penelitian yang dilakukan, teknologi yang cocok untuk implementasi *smart university* adalah ZigBee. Hal tersebut dikarenakan cakupan wilayah cukup luas sehingga ZigBee sesuai dengan spesifikasi yang diinginkan.

Daftar Pustaka

[1] Aqeel-ur-Rehman, Abu Zafar Abbasi, Zubair A. Shaikh. Building A Smart University using RFID Technology. *International Conference on Computer Science and Software Engineering*. 2008; pp: 641-644.

[2] V.Abinayaa, Anagha Jayan. Case Study on Comparison of Wireless Technologies in Industrial Applications. *International Journal of Scientific and Research Publications.* 2014 Volume 4, Issue 2: 1-4.

[3] A.S. Diallo, A. Wajdi, R.F. Olanrewaju, dan F. Sado. A Secure Authentication for Bluetooth Connection. *International Conference on Computer & Communication Engineering.* 2014; pp: 60-63.

[4] Aji Supriyanto. Tinjauan Teknis Teknologi Perangkat Wireless dan Standar Keamanannya. *Jurnal Teknologi Informasi DINAMIK*. Juli 2006; Volume XI, No. 2: 75-83.

[5] Jobina Mary Varghese, Nibi K V, Vijo T Varghese, dan Sethuraman Rao. A Survey of The State of The Art in ZigBee. *International Journal on Cybernetics & Informatics (IJCI)*. April 2015; Vol. 4, No. 2: 145-155.

[6] Omojokun G. Aju. A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges. *International Journal of Computer Applications (0975 – 8887)*. November 2015; Volume 130 – No.9: 47-55

[7] Loukas, G., Oke, G, Gelenbe, E. *Defending against Denial of Service in a Self-Aware Network: A Practical Approach*. NATO Symposium on Information Assurance for Emerging and Future Military Systems. Ljubljana, Slovenia.(2008).

[8] Anneleen Van Nieuwenhuyse, Mario Alves dan Anis koubaa. *Technical report on the use of the Zigbee protocol for wireless sensor networks*. Technical Report HURRAY-TR-060601, 2006

[9] Wawan. *Sistem Keamanan pada Jaringan Zigbee*. Departemen Teknik Elektro Institut Teknologi Bandung. Report number: 28489670. 2003.

[10] Doaa Abdel-Gaber Abdel-Aleem Ali. Near-Field Communication Technology and Its Impact in Smart University and Digital Library: Comprehensive Study. *Journal of Library and Information Sciences.* December 2015; Vol. 3, No. 2, pp: 43-77.

[11] Gustasari. Pengontroloan Sistem Akses Menggunakan Card RFID dan Web Berbasis Arduino. Skripsi. Tangerang: Undergraduate STMIK RAHARJA; 2015.

[12] Indri Neforawati, Muhammad Irdam Fareza dan Vida Juniarti. Rancang Bangun Aplikasi Sistem Informasi Monitoring Absensi Mahasiswa Politeknik Negeri Jakarta Menggunakan Teknologi NFC pada Android. *POLITEKNOLOGI*. 2015; VOL. 14 No. 2: 1-8.

[13] Ryan H. F. Kontu, Sherwin R. U. A. Sompie, ST.MT Alicia A. E. Sinsuw, ST.MT. Perancangan Sistem Pembaca Surat Tanda Nomor Kendaraan Dengan Teknologi NFC. *E-journal Teknik Elektro dan Komputer*. 2015; ISSN: 2301-8402.

ISBN: 978-602-60581-0-2