

**INTERNET OF THINGS: SEBUAH KAJIAN PADA
LINGKUNGAN SMART HOME**

Skripsi



oleh
ANDY WIJAYA BINARTO
22074202

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2018

INTERNET OF THINGS: SEBUAH KAJIAN PADA LINGKUNGAN SMART HOME

Skripsi



Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

ANDY WIJAYA BINARTO
22074202

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2018

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

INTERNET OF THINGS: SEBUAH KAJIAN PADA LINGKUNGAN SMART HOME

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 10 Januari 2018



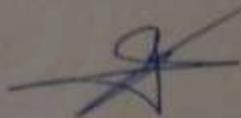
ANDY WIJAYA BINARTO
22074202

HALAMAN PERSETUJUAN

Judul Skripsi : INTERNET OF THINGS: SEBUAH KAJIAN PADA
LINGKUNGAN SMART HOME
Nama Mahasiswa : ANDY WIJAYA BINARTO
N I M : 22074202
Matakuliah : Skripsi (Tugas Akhir)
Kode : TIW276
Semester : Gasal
Tahun Akademik : 2017/2018

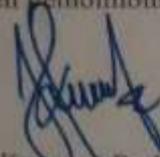
Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 29 November 2017

Dosen Pembimbing I



Willy Sudiarto Raharjo, S.Kom.,M.Cs.

Dosen Pembimbing II



Laurentius Kurnoro Probo Saputra,
S.T., M.Eng.

HALAMAN PENGESAHAN

INTERNET OF THINGS: SEBUAH KAJIAN PADA LINGKUNGAN SMART HOME

Oleh: ANDY WIJAYA BINARTO / 22074202

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 19 Desember 2017

Yogyakarta, 8 Januari 2018
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Laurentius Kuncoro Probo Saputra, S.T.,
M.Eng.
3. Antonius Rachmat C., S.Kom.,M.Cs.
- 4.



Dekan


(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi


(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul Internet of Things : Sebuah Kajian Pada Lingkungan Smart Home.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan pembuatan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terimakasih kepada::

1. **Bapak Willy Sudiarto Raharjo, S.Kom., M.Cs.** selaku dosen pembimbing pertama, yang telah banyak meluangkan waktunya untuk memberikan bimbingan, saran, ide, petunjuk serta masukan dan perbaikan sehingga penelitian ini dapat berjalan dengan lancar.
2. **Bapak Laurentius Kuncoro Probo Saputra, S.T., M.Eng.** selaku dosen pembimbing kedua yang telah sabar dan cermat untuk membimbing penulis sehingga penelitian ini dapat selesai dengan baik.
3. Ibu Gloria Virginia, S.Kom., MAI, PhD. selaku wakil dekan urusan akademik yang telah banyak memberikan kesempatannya bagi saya agar dapat menyelesaikan program studi strata I.
4. Dosen dosen Universitas Kristen Duta Wacana yang telah membantu.
5. Kedua orang tua saya yang selalu dengan sabar mendoakan dan mendukung saya untuk dapat menyelesaikan tulisan ini.
6. Teman teman gereja JKI Injil Kerajaan yang selalu setia mendukung saya agar saya dapat segera menyelesaikan tulisan ini.

Penulis menyadari bahwa laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari

pembaca sekalian sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

Akhir kata penulis ingi meminta maaf bila ada kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan sewaktu membuat Tugas Akhir ini. Sekali lagi penulis mohon maaf yang sebesar-besarnya dan semoga ini bermanfaat bagi kita semua.

Yogyakarta, 10 Januari 2018

Andy Wijaya Binarto

© U K D W

INTISARI

Penelitian ini dibatasi pada studi literatur tahun 2012-2017 tentang keamanan, *maintenance*, dan *update Internet Of Things* pada lingkungan *Smart Home*, serta membatasi pada rekomendasi dan implementasi dari *Internet Of Things*. Tujuan pada penelitian ini adalah: Untuk mengetahui keamanan IoT pada lingkungan *Smart Home*, untuk mengetahui kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor, untuk seberapa sering atau frekuensi *update* IoT pada lingkungan *Smart Home* dari pihak vendor, untuk mengetahui protokol komunikasi yang digunakan untuk berkomunikasi pada lingkungan *smart home*. Berdasarkan hasil analisis maka dapat disimpulkan bahwa: Keamanan IoT pada lingkungan *Smart Home* sudah baik. Hal ini dapat ditingkatkan dengan cara menggunakan *username* dan *password* khusus untuk menghindari *hacker* di masa mendatang. IoT pada lingkungan *Smart Home* dari pihak vendor sudah memiliki kesiapan *maintenance* dan sebaiknya dapat dipertahankan dimasa mendatang. *Maintenance* yang dilakukan pihak *vendor* terkait dengan *Smart Home* IoT selama ini cukup baik dimana dari Internet vendor akan secara teratur melakukan *update* sistem konfigurasi dan setelah itu pada tahap selanjutnya alat baru dengan *gateway* yang menyediakan ID *software* baru dipasang, setelah *gateway* menyediakan informasi *update service* kemudian alat atau perangkat lunak akan mengakses Internet untuk *update* di masa mendatang. Frekuensi *update* telah cukup baik dilakukan pada lingkungan *Smart Home* dari pihak vendor dalam setahun yaitu antara 1 hingga 10 kali, dan sebaiknya dapat dipertahankan dimasa mendatang. Hal ini disebabkan karena dengan adanya frekuensi *update* tersebut akan berdampak pada *update system* yang dipercaya oleh *user*. Protokol komunikasi digunakan dalam lingkungan *Smart Home* adalah BACnet, DNP3, EIB Eropa Instalasi Bus, LonWorks, Modbus, OPC – OLE, X-10 Protokol Residential, dan MQTT. *Open protokol* yang *secure* antara lain adalah Protokol MQTT dan TCP/IP.

KATA KUNCI: IOT, *Smart Home*

DAFTAR ISI

HALAMAN JUDUL.....	ii
PERNYATAAN KEASLIAN SKRIPSI.....	iii
HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
UCAPAN TERIMAKASIH.....	vi
INTISARI.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
BAB I: PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	8
1.3. Batasan Masalah.....	8
1.4. Tujuan Penelitian	8
1.5. Manfaat Penelitian	9
BAB II: LANDASAN TEORI.....	10
2.1. Penelitian Terdahulu	10
2.2. <i>Internet Of Things</i>	14
2.3. Sejarah <i>Internet of Things</i>	15
2.4. Aplikasi <i>Internet of Things</i>	17
2.5. IoT :Penelitian Strategis dan Inovasi Arah	18
2.6. Manfaat IoT	20
2.7. <i>Smart Home</i>	21
2.8. Keamanan IoT.....	24
2.9. <i>Maintenance IoT</i>	25
2.10. <i>Update IoT</i>	26
2.11. Protokol Komunikasi yang Digunakan untuk Melakukan Berkomunikasi ada IoT	26
2.12. <i>Internet of Things</i> Menurut CISCO	28
2.13. Kerangka Pikir	31

BAB III: METODOLOGI PENELITIAN	32
3.1. Jenis Penelitian.....	32
3.2. Jenis dan Sumber Data	33
3.3. Metode Pengumpulan Data.....	33
3.4. Teknik Analisis Data.....	33
BAB IV : HASIL ANALISIS DAN PEMBAHASAN	34
4.1. Keamanan IoT pada lingkungan <i>Smart Home</i>	34
4.2. Kesiapan <i>maintenance</i> IoT pada lingkungan <i>Smart Home</i> dari pihak vendor	39
4.3. Frekuensi <i>update</i> IoT pada lingkungan <i>Smart Home</i> dari pihak vendor .	41
4.4. Protokol komunikasi yang digunakan dalam lingkungan <i>Smart Home</i> ...	45
BAB V: PENUTUP	49
5.1. Kesimpulan	49
5.2. Saran	50
5.3. Keterbatasan.....	50
DAFTAR PUSTAKA	51
LAMPIRAN	

DAFTAR TABEL

Tabel 2.1. <i>Smart HomeApplication</i>	23
Tabel 4.1. Protokol komunikasi 1 dan 2 arah.....	48

©UKDW

DAFTAR GAMBAR

Gambar 2.1. IoT Ekosistem	19
Gambar 2.2. <i>Internet Of Things</i>	20
Gambar 2.3. Konsep <i>Smart Home System</i>	22
Gambar 2.4. Kerangka Pikir.....	31
Gambar 4.1. Garis waktu serangan kode Mirai.....	36
Gambar 4.2. <i>Update</i> dari IoT <i>Smart Home</i>	42
Gambar 4.3. Jawaban dari Creston tentang <i>update</i>	43
Gambar 4.4. Jawaban dari AMX tentang <i>update</i>	44

©UKDWN

INTISARI

Penelitian ini dibatasi pada studi literatur tahun 2012-2017 tentang keamanan, *maintenance*, dan *update Internet Of Things* pada lingkungan *Smart Home*, serta membatasi pada rekomendasi dan implementasi dari *Internet Of Things*. Tujuan pada penelitian ini adalah: Untuk mengetahui keamanan IoT pada lingkungan *Smart Home*, untuk mengetahui kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor, untuk seberapa sering atau frekuensi *update* IoT pada lingkungan *Smart Home* dari pihak vendor, untuk mengetahui protokol komunikasi yang digunakan untuk berkomunikasi pada lingkungan *smart home*. Berdasarkan hasil analisis maka dapat disimpulkan bahwa: Keamanan IoT pada lingkungan *Smart Home* sudah baik. Hal ini dapat ditingkatkan dengan cara menggunakan *username* dan *password* khusus untuk menghindari *hacker* di masa mendatang. IoT pada lingkungan *Smart Home* dari pihak vendor sudah memiliki kesiapan *maintenance* dan sebaiknya dapat dipertahankan dimasa mendatang. *Maintenance* yang dilakukan pihak *vendor* terkait dengan *Smart Home* IoT selama ini cukup baik dimana dari Internet vendor akan secara teratur melakukan *update* sistem konfigurasi dan setelah itu pada tahap selanjutnya alat baru dengan *gateway* yang menyediakan ID *software* baru dipasang, setelah *gateway* menyediakan informasi *update service* kemudian alat atau perangkat lunak akan mengakses Internet untuk *update* di masa mendatang. Frekuensi *update* telah cukup baik dilakukan pada lingkungan *Smart Home* dari pihak vendor dalam setahun yaitu antara 1 hingga 10 kali, dan sebaiknya dapat dipertahankan dimasa mendatang. Hal ini disebabkan karena dengan adanya frekuensi *update* tersebut akan berdampak pada *update system* yang dipercaya oleh *user*. Protokol komunikasi digunakan dalam lingkungan *Smart Home* adalah BACnet, DNP3, EIB Eropa Instalasi Bus, LonWorks, Modbus, OPC – OLE, X-10 Protokol Residential, dan MQTT. *Open protokol* yang *secure* antara lain adalah Protokol MQTT dan TCP/IP.

KATA KUNCI: IOT, *Smart Home*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi informasi dan komunikasi di era globalisasi merupakan sebuah fenomena yang memberikan tantangan besar bagi perusahaan untuk terus bertumbuh dan berkembang. Berbagai perusahaan terus menyesuaikan diri, baik dari segi produk, layanan, dan strategi pemasarannya untuk mampu bersaing di dalam pasarnya masing-masing. Khususnya di bidang jasa telekomunikasi, perusahaan dituntut untuk terus memberikan layanan yang terbaik demi menjaga stabilitas perusahaan sekaligus mendapatkan keuntungan sebesar-besarnya. Angka pengguna *smartphone* di Indonesia yang terus bertumbuh dan trend “*Internet Of Things*” merupakan sebuah pertanda akan adanya potensi yang sangat besar di pasar Indonesia. Mayoritas individu di kota besar di Indonesia saat ini sangat bergantung pada penggunaan *smartphone* dalam menjalankan aktifitas sehari-hari. Penggunaan teknologi *smartphone* tentunya beriringan dengan pemakaian data dan Internet dari penggunanya.

Penggunaan komputer dimasa datang akan mendominasi pekerjaan manusia dan mengalahkan kemampuan komputasi manusia seperti penggunaan peralatan elektronik dari jarak jauh, menggunakan media Internet, IoT (*Internet Of Things*). Hal tersebut memungkinkan pengguna untuk mengelola dan mengoptimalkan peralatan elektronik yang menggunakan Internet. Hal ini mengindikasikan bahwa dalam waktu dekat

komputer dan peralatan elektronik mampu bertukar informasi melalui sarana tersebut, sehingga mengurangi interaksi pertemuan manusia secara langsung. Hal ini juga akan membuat jumlah pengguna Internet semakin meningkat dengan berbagai fasilitas dan layanan Internet. Tantangan utama dalam IoT adalah menjembatani kesenjangan antara dunia fisik dan dunia informasi, seperti bagaimana mengolah data yang diperoleh dari peralatan elektronik melalui sebuah *interface* antara pengguna dan peralatan itu. Sensor mengumpulkan data mentah fisik dari skenario *real time* dan mengkonversikan ke dalam mesin format yang dimengerti sehingga akan mudah dipertukarkan antara berbagai bentuk format data.

"Things" pada *Internet of Things* dapat didefinisikan sebagai subjek misalkan orang dengan monitor *implant* jantung, hewan peternakan dengan transponder *biochip*, sebuah mobil yang telah dilengkapi *built-in* sensor untuk memperingatkan pengemudi ketika tekanan ban rendah. Sejauh ini, IoT paling erat hubungannya dengan komunikasi *machine-to-machine* (M2M) di bidang manufaktur dan listrik, perminyakan, dan gas. Dengan semakin berkembangnya infrastruktur Internet, maka menuju tahap selanjutnya adalah tahap di mana bukan hanya *smart phone* atau komputer saja yang dapat terkoneksi dengan Internet. Namun berbagai macam benda nyata akan terkoneksi dengan Internet. *Internet of Things* (IoT), kadang-kadang disebut sebagai Internet dari *Objects*, yang akan berubah segala sesuatunya atau objek yang selalu berubah. Hal ini menyatakan bahwa dampak Internet yang begitu besar di berbagai bidang termasuk bidang

pendidikan, komunikasi, bisnis, ilmu pengetahuan, pemerintah, dan kemanusiaan. Internet adalah salah satu yang paling penting dan kuat dalam sejarah manusia. Sekarang dapat dikatakan bahwa IoT merupakan evolusi berikutnya dari Internet, mampu menganalisis dan mendistribusikan data menjadi informasi, pengetahuan, dan teknologi. Dalam konteks ini, IoT menjadi sangat penting.

Rumah dapat berfungsi sebagai tempat untuk menikmati kehidupan yang nyaman, tempat untuk beristirahat, tempat berkumpulnya keluarga dan tempat untuk menunjukkan tingkat sosial dalam masyarakat. Rumah sebagai tempat tinggal harus dibuat se nyaman mungkin agar membuat penghuninya merasa betah. Selain itu rumah juga harus bisa membuat penghuninya merasa aman dan nyaman tinggal di dalamnya. Di zaman yang serba modern seperti sekarang, rumah bisa menjadi sangat bersahabat dengan penghuninya. Misalnya rumah cerdas atau yang biasa disebut *Smart Home*, merupakan rumah yang dilengkapi dengan sistem pengoperasian terkontrol untuk banyak hal seperti pencahayaan lampu, barang-barang elektronik, serta benda-benda yang bisa diberi motor penggerak seperti gorden, pintu garasi, pintu pagar dan sebagainya. Dengan pengaturan *on* dan *off* atau buka dan tutup melalui sebuah atau beberapa outlet semacam *remote control*.

Smart Home adalah suatu rumah yang dilengkapi dengan sistem untuk mengintegrasikan dan mengontrol alat-alat elektronik yang ada di rumah, misalnya Lampu, TV, *Home Theater*, CCTV, Alarm, Kipas angin, *Door Lock*, *Motion Sensor*, dan masih banyak lagi. Tujuan dari sistem

Smarthome mencakup kemudahan, efisiensi energi, keamanan, dan kenyamanan. Saat ini popularitas tentang konsep *Home Automation* sedang berkembang pesat, dan didukung dengan banyaknya perusahaan yang bergerak dibidang ini seperti Control, Crestron, AMX, KNX, Dynalite, dan lain-lain, sistem *Smart home* terbagi pada beberapa bagian di antaranya adalah *Smarthome* pada *lighting control*, yaitu sebuah sistem pencahayaan yang dirancang dengan baik dan sistem kontrol pencahayaan dapat beroperasi sebagai inti dari sistem otomatisasi berbagai rumah yang digunakan dalam rumah pintar (*Smart Home*). Penggunaan energi listrik pada setiap rumah menjadikan hal yang terpenting karena dalam penggunaan listrik yang tidak dibutuhkan dapat mengakibatkan pemborosan energi listrik.

Pemerintah pada saat ini mengalami salah satu masalah yang serius dalam kejahatan yaitu *Cybercrime*. *Cybercrime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama, *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya Internet. Di Negara-negara maju kasus kejahatan seperti ini juga marak tidak hanya terjadi seperti di Amerika dan Eropa namun juga di Negara berkembang yang ada di Asia dan Afrika. Maka dari itu keamanan IoT pada lingkungan *smart home* hal penting untuk diperhatikan dan dianalisis.

Malware merupakan suatu program yang diciptakan oleh seseorang dengan tujuan tertentu, namun biasanya dalam penggunaannya, malware digunakan dengan tujuan untuk mengubah, merusak, bahkan mencuri data

yang dimiliki oleh korban sehingga pelaku dapat menggunakan data yang didapatnya dengan tidak bertanggungjawab. Tidak ada data akurat mengenai asal mula *malware* diciptakan, namun pada tahun 1983 virus komputer modern pertama kali dicetuskan dan disampaikan oleh Fred Cohen, seorang mahasiswa pascasarjana USC. Pada November 1983, Cohen mendokumentasikan virus pertama kali, yaitu virus komputer yang dapat mereplika diri sendiri dengan meng-*inject* program virus terhadap “*host*” program atau dokumen.

Pada umumnya *user* hanya tahu akibat dari serangan *malware* tersebut. Kebanyakan mereka mengetahui setelah komputernya terserang oleh program *malware* dan segera mencari *software* anti virus yang dapat menghapus dan menghentikan serangan tersebut. Mereka tidak ingin tahu kenapa *malware* tersebut bisa menyerang, bagaimana *malware* tersebut bisa berkembang atau memanipulasi dirinya sendiri, bagaimana *malware* tersebut bisa lolos dari program atau *software* anti virus yang sudah dipasang atau ter-*install*, bagaimana cara penanganan dan pencegahan yang baik agar *malware* tersebut tidak kembali lagi, dan perkembangan *malware* sekarang ini serta sejauh mana efek atau dampak yang ditimbulkan dari program *malware* sekarang ini dibandingkan program *malware* sebelumnya.

Salah satu jenis *Malware* berbahaya bagi IoT adalah *Malware* Mirai. Kode sumber Mirai telah dirilis oleh pembuatnya di sebuah situs forum peretas. Di dalam kode sumber tersebut, terdapat daftar kata sandi beserta

nama pengguna yang digunakan sebagai pembuka pintu akses perangkat IoT seperti kamera, DVR, *Router* dan sebagainya yang tergabung di dalam sebuah jaringan. Pada umumnya, perangkat IoT mempunyai nama pengguna dan kata sandi yang telah dirancang secara *default* dari pabrik. Celah inilah yang dimanfaatkan oleh Mirai. Dengan memanfaatkan *default setting* dari perangkat IoT, Mirai akan merangsek masuk ke dalam jaringan kemudian menyebar untuk melakukan *scanning* via Telnet. Setelah itu, pasukan zombie botnet akan memenuhi jaringan. Traffic yang dipadati oleh Mirai dapat mencapai angka 620 Gbps, namun angka ini dapat lebih tinggi jika tidak diantisipasi. Dalam menjalankan operasinya, Mirai memanfaatkan dua akun VPS. Satu VPS digunakan sebagai Command and Control (C&C), sedangkan yang lain digunakan untuk load balancing. Hal ini membuat Mirai bekerja dengan terorganisir dan cepat dalam menentukan turun dan naiknya arus *traffic* korban. Serangan Mirai dapat diantisipasi dengan cara melakukan *reboot* pada sistem. Namun, para ahli menyatakan bahwa *reboot* tidak memberantas Mirai, hanya menahan serangan untuk sementara. Karena dalam hitungan menit, Mirai dapat mengerahkan pasukannya kembali. Opsi lain untuk menghentikan serangan Mirai adalah dengan mengganti kata sandi default pada perangkat IoT (Inna, 2016).

Penelitian *Smart Home* sangat diperlukan karena seiring dengan makin berkembangnya zaman, teknologi juga akan semakin tumbuh dengan pesat. Sistem *smart home* memiliki banyak keuntungan dan berbagai fasilitas yang tentunya akan dapat memberikan keamanan dan kenyamanan bagi

pemilik rumah dan orang-orang yang tinggal di dalamnya, karena dapat memudahkan pekerjaan agar menjadi lebih cepat, efektif dan efisien. Harapan positif dari perkembangan *Internet of Things* adalah agar tata kehidupan manusia akan menjadi lebih mudah, lebih nyaman, lebih aman, lebih teratur, dan lebih sehat. Hal-hal yang akan dikaji dalam penelitian ini yaitu keamanan IoT, *maintenance* IoT, frekuensi *update* IoT dan protokol yang digunakan pada lingkungan *smart home*.

Kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor juga merupakan hal penting untuk diteliti karena jika tidak ada *maintenance* yang optimal akan berbahaya bagi pengguna IoT. Selain itu, seberapa sering atau frekuensi *update* IoT pada lingkungan *Smart Home* dari pihak vendor juga penting karena jika tidak ada *update* maka kejahatan di dunia maya semakin tinggi. Protokol komunikasi yang digunakan dalam lingkungan *Smart Home* adalah hal penting karena dengan adanya protokol yang baik akan mengoptimalkan komunikasi antara vendor dengan *user*.

Maka berdasarkan pada uraian tersebut penelitian ini dengan judul "*Internet Of Things: Sebuah Kajian pada lingkungan Smart Home*".

1.2. Rumusan Masalah

Kesiapan dunia industri dalam mengimplementasikan teknologi IoT pada *Smart Home* adalah hal yang penting, maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana keamanan IoT pada lingkungan *Smart Home*?
2. Bagaimana kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor?
3. Seberapa sering atau frekuensi *update* IoT pada lingkungan *Smart Home* dari pihak vendor?
4. Protokol komunikasi apakah yang digunakan dalam lingkungan *Smart Home*?

1.3. Batasan Masalah

Penelitian ini dibatasi pada studi literatur tahun 2012-2017 tentang keamanan, *maintenance*, dan *update Internet Of Things* pada lingkungan *Smart Home*, serta membatasi pada rekomendasi dan implementasi dari *Internet Of Things*

1.4. Tujuan Penelitian

Tujuan pada penelitian ini adalah:

1. Untuk mengetahui keamanan IoT pada lingkungan *Smart Home*.

2. Untuk mengetahui kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor.
3. Untuk seberapa sering atau frekuensi *update* IoT pada lingkungan *Smart Home* dari pihak vendor.
4. Untuk mengetahui protokol komunikasi yang digunakan untuk berkomunikasi pada lingkungan *Smart home*.

1.5. Manfaat Penelitian

a. Manfaat praktis

Secara praktis, hasil dari penelitian ini diharapkan dapat menjadi masukan bagi semua pihak yang membaca penelitian ini agar dapat memperluas konsep Internet. Dan bagi pihak lain penelitian ini juga diharapkan dapat membantu pihak lain dalam penyajian informasi untuk mengadakan penelitian serupa.

b. Manfaat teoritis

Secara teoritis, hasil dari penelitian ini diharapkan dapat menjadi referensi atau masukan bagi perkembangan ilmu informatika untuk mengetahui keamanan, kesiapan *maintenance*, frekuensi update dan protokol yang digunakan pada lingkungan *Smart Home*.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis maka dapat disimpulkan bahwa:

1. Keamanan IoT pada lingkungan *Smart Home* sudah baik. Hal ini dapat ditingkatkan dengan cara menggunakan *username* dan *password* khusus untuk menghindari *hacker* di masa mendatang.
2. Kesiapan *maintenance* IoT pada lingkungan *Smart Home* dari pihak vendor sudah cukup baik semoga dapat dipertahankan di masa mendatang. *Maintenance* yang dilakukan pihak *vendor* terkait dengan *Smart Home* IoT adalah vendor akan secara teratur melakukan *update* sistem konfigurasi dan setelah itu pada tahap selanjutnya alat baru dengan *gateway* yang menyediakan ID *software* baru dipasang, setelah *gateway* menyediakan informasi *update service* kemudian alat atau perangkat lunak akan mengakses Internet untuk *update* di masa mendatang.
3. Pada frekuensi *update* , tidak ada patokan waktu yang spesifik dari masing-masing vendor untuk melakukan *update firmware*, apabila tersedia *update firmware* yang terbaru maka akan ada notifikasi atau pemberitahuan kepada *user* agar segera melakukan *update firmware* yang terbaru. Namun ada juga vendor yang tidak akan melakukan banyak *update* pada *firmware*-nya karena mereka merasa *firmware*

awal yang mereka berikan kepada *user* sudah dirancang untuk memberikan kualitas dan fitur yang terbaik.

4. Protokol komunikasi digunakan dalam lingkungan *Smart Home* adalah BACnet, DNP3, EIB Eropa Instalasi Bus, LonWorks, Modbus, OPC – OLE, X-10 Protokol Residential, dan MQTT. *Open protokol* yang *secure* antara lain adalah Protokol MQTT dan TCP/IP.

5.2 Saran

Saran untuk penelitian ini adalah:

1. Sebaiknya IoT dapat ditingkatkan dan dikembangkan lebih baik lagi.
2. Pada penelitian serupa dimasa mendatang dapat ditambahkan penyebaran kuesioner untuk mengetahui tanggapan responden terhadap IoT atau menggunakan analisis kuantitatif, menggunakan survey sosial untuk mengetahui persepsi pengguna IoT di masyarakat.

5.3 Keterbatasan

Penelitian ini memiliki keterbatasan antara lain adalah: masih terbatasnya data mengenai frekuensi *update* dari masing-masing vendor yang ada, sehingga analisis untuk frekuensi *update* IoT tidak maksimal dan kurang mendetail.

DAFTAR PUSTAKA

- Arikunto, S. (2010). *Prosedur Penelitian Suatu Pendekatan Praktek*. Jakarta: Penerbit Rineka Cipta.
- Ashton, K. (2009). That “Internet of Things” Thing. *RFID Journal*.
- Bhide, V. H. (2014). A Survey on the Smart Homes using Internet of Things (IoT), 243–246.
- Bregman, D. (2010). Smart Home Intelligence-The eHome that Learns. *International Journal of Smart Home*, 4(4).
- Bregman, D., & Korman, A. (2009). A Universal Implementation Model for the Smart Home. *International Journal of Smart Home*, 3(3).
- Davidovic, B., & Labus, A. (2016). A smart home system based on sensor technology. *Facta Universitatis - Series: Electronics and Energetics*, 29(3), 451–460. <https://doi.org/10.2298/FUEE1603451D>
- Davies, R. (2015). The Internet of Things Opportunities and challenges. *Members’ Research Service*, (May), 6. <https://doi.org/10.5480/1536-5026-34.1.63>
- Evans, D. (2012). The Internet of Things - How the Next Evolution of the Internet is Changing Everything. *Cisco Internet Business Solutions Group (IBSG)*, (April), 1–11. <https://doi.org/10.1109/IEEESTD.2007.373646>
- Farooq, M. U., & Waseem, M. (2015). A Review on Internet of Things (IoT). *International Journal of Computer Applications (0975 8887)*, 113(1), 1–7.
- Gondaliyal, T. (2016). Sensor communication in Smart Home Using IoT. *International Institution for Technological Research and Development*.
- Inna, R.A. (2016). *Mirai, Ancaman via IoT. ICISA, Infortion and Cyber Security Awareness*. <https://kami.kominfo.go.id>.
- Li, S., Xu, L. Da, & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17(2), 243–259. <https://doi.org/10.1007/s10796-014-9492-7>
- Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3), 44. <https://doi.org/10.3390/info7030044>
- Lindsay, G., Woods, B., & Corman, J. (2016). *Smart Homes and the Internet of Things*. Atlantic Council.
- Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review, 3(May), 164–173.

- Pandikumar, S., & Vetrivel, R. S. (2014). Internet of Things Based Architecture of Web and Smart Home Interface Using GSM. *International Journal of Innovative Research in Science, Engineering and Technology*, 3(3).
- Ravi Kumar, K., & Akbar, S. (2014). Android Application Based Real Time Home Automation. *Indian Journal Of Applied Research*, 4(7), 188–190.
- Ron Weber, H., & Romana Weber. (2010). *Internet of Things*. Springer: Verlag Berlin Heidelberg.
- Safaat, N. (2011). *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung: CV. Informatika.
- Satria, A., Luthfi Priadi, M., Ayu Wulandhari, L., & Widodo. (2015). The Framework of Home Remote Automation System Based on. *International Journal of Smart Home*, 9(1), 53–60.
- Schmidt, A.-D., Peters, F., Lamour, F., Scheel, C., Camtepe, S. A., & Albayrak, S. (2009). Monitoring Smartphones for Anomaly Detection. *Mobile Networks and Applications*, 14(1), 92–106.
- Steven, G. (2010). *Smart Home Automation with Linux. ISBN-13 (Electronic): 978-1-4302-2779-3, Apress*.
- Tjakrawidjaj, A. H. (2006). Growth of Bonytongue Fish (Scleropages jardinii Saville-Kent) in Aquarium. *Jurnal Iktiologi Indonesia*, 6(1), 61–65.
- Vermesan, O., & Peter Friess. (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publisher. Retrieved from <http://www.kisa.or.kr/uploadfile/201306/201306101740531675.pdf>
- Yurmama S., T. F., & Azman, N. (2009). Perancangan Software Aplikasi Pervasive Smart Home. *Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta*.