Penggunaan Distribusi Kunci Diffie-Hellman untuk Penerapan Aspek Privacy pada Automatic Meter Reading (AMR)

Vera Suryani*,
Jurusan Teknik Elektro dan Teknologi Informasi,
Universitas Gadjahmada, Yogyakarta
*Fakultas Informatika
Universitas Telkom
Bandung - Indonesia
vera.s3te14@mail.ugm.ac.id

Selo[1], Widyawan[2]
Jurusan Teknik Elektro dan Teknologi Informasi,
Universitas Gadjahmada, Yogyakarta
{[1]selo@ugm.ac.id, [2]widyawan@ugm.ac.id}

***Abstrak*— Teknologi Automatic Meter Reading (AMR) sebagai salah satu cikal bakal teknologi yang dapat dikembangkan di IoT, dimana AMR belum banyak yang dilengkapi dengan proteksi untuk *privacy*. Banyak cara dapat digunakan untuk menerapkan aspek *privacy* di AMR, salah satunya adalah menggunakan algoritma untuk mengamankan kunci dan mengenkripsi data. Pada paper ini dilakukan penerapan *privacy* berupa penggunaan distribusi kunci Diffie-Hellman dan enkripsi data penggunaan listrik diperumahan berbasis algoritma *Rivest Shamir Adleman* (RSA). Melalui simulasi di Matlab, kedua algorima tersebut di bangkitkan untuk di analisis lebih lanjut pengaruhnya terhadap panjang kunci dan waktu *refreshment* kunci. Hasil simulasi menunjukkan bahwa waktu *refreshment* kunci lebih berpengaruh dibandingkan dengan panjang kunci. Dan penggunaan kunci sepanjang 1024 bit dengan periode *refreshment* per 24 jam paling optimal dibandingkan dengan panjang kunci yang lebih pendek dengan waktu refreshment lebih sering.**

Kata kunci : AMR, IoT, privacy, Diffie-Hellman, RSA

I.PENDAHULUAN

Sistem terdistribusi didefinisikan sebagai sistem yang terdiri dari hardware maupun software yang terhubung melalui jaringan komputer, komponen-komponen tersebut saling berkomunikasi untuk mempertukarkan data [1].

Perkembangan sistem terdistribusi saat ini sangat pesat. Tak hanya jenis *software* dan *hardware* yang lebih beragam mulai dari sensor hingga *smartphone*, namun macam jaringan pun semakin bervariasi. Mulai dari jaringan yang bersifat lokal seperti *Wireless Sensor Network* (WSN), *cloud network*, hingga yang memanfaatkan jaringan Internet untuk koneksinya seperti *Internet of Things*.

Ide dasar dari *Internet of Things* adalah menyediakan komunikasi dan layanan tanpa batas antar objek atau *things*. Objek dapat berupa sensor, aktuator, *smart phones*, berinteraksi dan bekerja sama satu sama lain memungkinkan untuk terwujudnya IOT yang dapat membuat layanan yang lebih baik dan dapat diakses kapan saja, dari mana saja [2]

IoT dapat diterapkan diberbagai aplikasi seperti *smart environtment*, transportasi dan logistik, *e-health*, dan lain sebagainya [14]. Contoh penerapan pada *smart environment* adalah *smart metering* pada perhitungan daya listrik atau *Automatic Meter Reading* (AMR) diperumahan. AMR memungkinkan perusahaan penyedia jasa listrik untuk memantau penggunaan listrik di setiap rumah secara online melalui Internet. Dengan demikian tidak diperlukan lagi petugas yang berkeliling diperumahan untuk mencatat jumlah daya yang dikonsumsi per rumah. Bahkan data yang diterima tersebut dapat diolah dan dianalisis lebih lanjut jika terjadi pencurian daya listrik.

Mengingat IoT memanfaatkan jaringan Internet secara umum, maka banyak tantangan yang muncul disana. Menurut hasil survey [3] dikemukakan bahwa beberapa *device* atau *objects* memiliki *software* dan OS tersendiri sehingga menyulitkan proses integrasi di IoT. Tantangan lainnya yang muncul adalah masalah keamanan [4][5][6]. Secara spesifik, pada aplikasi smart metering ditemukan tantangan yang terkait dengan *privacy* [7]. Dari implementasi AMR [15] didapatkan hasil bahwa diperlukan pengamanan terkait aspek *privacy* agar pengiriman data pelanggan tidak disalahgunakan. Pentingnya penanganan privacy di AMR dapat juga ditemukan di [16].

Berdasarkan Internet security glossary [13], privacy didefinisikan sebagai *"the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others"*.

Aspek privacy dapat diimplementasikan di sisi device, network, dan aplikasi [8]. Cukup banyak penelitian yang membahas tentang aspek privacy di sisi network dengan mengembangkan protokol yang sebelumnya sudah ada di Internet seperti PANA [5], 6LoWPAN dan IPSec [9], HIP [10]. Sedangkan di sisi aplikasi, pemanfaatan protocol HTTPS [11]

dan penerapan *policy* untuk pembuatan desain produk atau aplikasi IoT dari European Union [12].

Belum banyak penelitian yang membahas mengenai implementasi *privacy* di IoT dari sisi *device*, terutama yang terkait dengan smart metering. *Privacy smart metering* menjadi penting mengingat data yang dikirimkan rentan terhadap manipulasi oleh pihak tertentu, yang salah satu efeknya adalah kasus pencurian listrik.

Aspek privacy pada AMR dapat diimplementasikan dengan cara membatasi akses ke *device* hanya untuk pengguna tertentu saja. Salah satu cara yang dapat digunakan adalah dengan memanfaatkan algoritma kriptografi tertentu beserta pertukaran kunci yang sesuai dengan karakteristik IoT. Pemilihan algoritma kriptografi dan skema distribusi kunci yang bersifat green akan menjadi penentu performansi dari AMR di IoT.

Dalam paper ini akan dibahas penggunaan kunci distribusi Diffie-Hellman untuk menerapkan aspek privacy di AMR yang digunakan diperumahan. Algoritma enkripsi yang digunakan adalah *Rivest Shamir Adleman* (RSA). Secara khusus akan digunakan studi kasus pengiriman data penggunaan listrik dari *Automatic Meter Reading.* Diharapkan nantinya penelitian ini akan dapat memberikan kontribusi untuk pengamanan monitoring penggunaan dan penghematan listrik, serta dapat mengurangi pencurian listrik. Selain itu, dari paper ini diharapkan mampu memberikan rekomendasi untuk pemilihan panjang kunci yang ideal untuk proses authentikasi dan enkripsi pada lingkungan AMR.

II. Automatic Meter Reading

Automatic Meter Reading (AMR) merupakan teknologi untuk mengumpulkan data metering dari air, gas, listrik, dll. secara otomatis untuk dikirimkan ke basisdata sentral guna diolah lebih lanjut [19]. Pengolahan data AMR salah satunya adalah untuk keperluan *billing* dan pencegahan terhadap pencurian data. AMR memiliki beberapa keuntungan : akurasi data metering, mempermudah proses *billing*, meminimalisasi *human error*, dan mempermudah proses *maintenance.*

Komponen AMR terdiri dari hal [19] :

a. Modul untuk metering
   Berupa power supply, sensor meter, dan antarmuka dari sensor agar dapat berkomunikasi secara jarak jauh ke server/basisdata sentral.
b. Sistem komunikasi
   Digunakan untuk proses transmisi data yang dihasilkan sensor; bisa berupa jalur telepon, *powerline carrier* (PLC), frekuensi radio (RF).
c. Peralatan pengolahan data di server/basisdata sentral
   Terdiri dari modem, komputer, data konsentrator, dll.

Gambar 1. Arsitektur Sistem

Secara umum system di AMR dapat digambarkan seperti yang tertera pada gambar 1.

III. Distribusi Kunci Diffie-Hellman

Distribusi kunci Diffie-Hellman merupakan algoritma pertukaran kunci simetris yang digunakan oleh dua pihak untuk mendapatkan kesepakatan mengenai kunci yang akan digunakan dalam proses pertukaran data nantinya [17].

Algoritma ini dipublikasikan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976. Data yang dibutuhkan dalam algoritma dipertukarkan melalui jaringan publik. Proses yang dilakukan oleh algoritma ini adalah sebagai berikut :

1. Perlu kesepakatan antara kedua pihak yang akan berkomunikasi, misalkan Alice dan Bob untuk memilih bilangan prima yang besar, yaitu n dan g, sedemikian sehingga $g < n$
2. Alice membangkitkan bilangan bulat acak yang cukup besar x dan mengirim hasil perhitungan matematis A berikut ini kepada Bob :
$$A = g^x \bmod n \quad (1)$$
3. Bob membangkitkan bilangan bulat acak yang cukup besar y dan mengirim hasil perhitungan matematis B berikut ini kepada Alice :
$$B = g^y \bmod n \quad (2)$$
4. Alice menghitung :
$$K = B^x \bmod n \quad (3)$$
Hasil perhitungan K dikirimkan ke Bob
5. Bob menghitung :
$$K' = A^y \bmod n \quad (4)$$
Hasil perhitungan K' dikirimkan ke Alice
6. Baik Alice maupun Bob akan membandingkan nilai K dan K' . Jika $K = K'$ maka telah didapatkan kunci simetris antara Bob dan Alice.

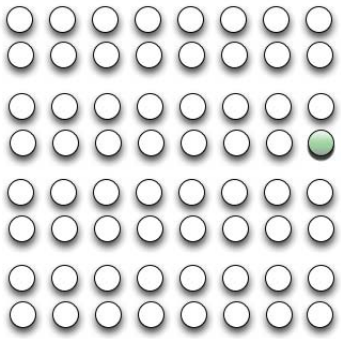
Seseorang yang menyadap pembicaraan antara Alice dan Bob dimungkinkan memiliki informasi n, g, A, B, namun ia tidak memiliki informasi nilai x dan y. Dengan demikian ia tidak akan dapat menghitung nilai K.

Nilai x dan y sangat sulit diketahui, kecuali dengan perhitungan logaritma diskrit.

IV. Pemodelan Sistem

Sistem yang dibuat berbentuk simulasi menggunakan alat bantu Matlab. Arsitektur system dapat dilihat pada gambar 1. Node yang berkomunikasi merupakan sensor untuk mengukur kWh yang berjumlah 64 buah. Sensor bertugas melakukan authentikasi dan mencatat jumlah daya yang digunakan pada setiap rumah di perumahan, dengan penempatan seperti yang terlihat pada gambar 2, dimana lingkaran berwarna putih adalah sensor, dan lingkaran berwarna hijau adalah server.

Jarak antar sensor secara horizontal adalah 8 meter, sedangkan jarak secara vertical adalah 20 meter. Setiap sensor hanya dapat berkomunikasi dengan sensor lainnya secara vertikal atau horizontal yang bertetanggaan, dan tidak secara miring. Perumahan merupakan area dengan dimensi 150 x 200 meter. Server dimodelkan dengan sebuah PC yang memiliki prosesor berkecepatan 2.5 GHz prosesor dan daya 60 Watt.



Gambar 2. Topologi Penempatan Sensor

Panjang kunci yang digunakan untuk proses authentikasi bervariasi, seperti yang terlihat pada tabel 1.

Tabel 1. Variasi panjang kunci dan waktu *refreshment* kunci

No	Panjang Kunci (bit)	Waktu *refreshment* (jam)
1.	128	1
2.	256	6
3.	512	12
4.	1024	24

Setiap sensor dimodelkan dapat berkomunikasi dengan sensor lainnya menggunakan jaringan Zigbee. Zigbee dipilih karena sifatnya yang *low power energy*, dengan daya jangkau hingga puluhan meter dan *transfer rate* sebesar 250 kbit/sec. Karakteristik Zigbee ini sangat sesuai dengan model komunikasi antara node dengan server di AMR. Antenna yang digunakan bersifat *omnidirectional*. Sensor yang dimodelkan dengan prosesor berjenis Atmel ATmega1281 yang memiliki frekuensi *clock* 16 MHz [18].

Antar sensor berkomunikasi secara *ad hoc* menuju server menggunakan routing protocol *Ad Hoc On-Demand Distance Vector* (AODV). AODV merupakan protokol ruting yang bersifat *on-demand*, yaitu hanya mengirimkan pesan jika dibutuhkan saja. Dengan demikian routing protocol ini tidak terlalu memberatkan sensor pada saat mengirimkan pesan.

Proses komunikasi antara sensor dan server terjadi secara periodik seperti yang tercantum pada tabel 1. Untuk menjaga proses komunikasi dapat selalu dilakukan meskipun listrik sedang mati, maka sensor memanfaatkan batere untuk sumber energi dalam proses komunikasi dengan server tersebut.

Energi pada sensor dimodelkan dengan penyesuaian terhadap datasheet dari Memsic IRIS [18]. Pada [18] dispesifikasikan bahwa node membutuhkan 8 μA pada saat *sleep*, 8 mA saat *idle*, 16 mA saat *receive* (Rx), dan 17 mA saat *transmit* (Tx). Setiap node diberikan *initial energy* setara dengan 2 baterei AA. Setiap baterei AA memiliki tegangan sebesar 1.5 volt, dengan kapasitas sebesar 1800-2600 mAh.
Selama proses pertukaran kunci, setiap node dapat melakukan proses *transmit, receive, idle,* maupun *sleep.* Untuk mendapatkan energi yang digunakan saat *transmit, receive, idle,* maupun *sleep* maka diperlukan besaran data, dalam hal ini adalah panjang kunci yang dikirimkan. Perhitungan waktu transmit untuk mengirimkan 128 bit kunci adalah sebagai berikut :

$$t_k = \frac{k}{r} \quad , \tag{5}$$

dengan k adalah besar data (bit), dan r adalah transfer rate (bps).
Untuk mencari energi yang diperlukan untuk mentransmisikan kunci sebesar 128 bit:

$$E_{TX} = V(volt) \times I(A) \times t_k \tag{6}$$

dengan V adalah tegangan, I adalah arus, dan t_{TX} adalah waktu transmit.
Dari persamaan (5) didapatkan nilai t_{TX} = 128/250.10^3 = 0.512 ms. Dan nilai E_{TX} adalah 1.5 V x 17 mA x 0.512 ms = 13.056 μJ. Dengan cara yang didapatkan nilai E_{RX} adalah 12.288 μJ, E_{idle} dan E_{sleep} adalah 6.144 μJ.
Parameter yang digunakan untuk menguji sistem adalah waktu total untuk authentikasi dan energi yang dikonsumsi oleh node pada saat authentikasi. Total waktu authentikasi yang dibutuhkan oleh sensor berdasarkan persamaan (1) s.d (4) dihitung dengan cara :

$$t_{auth} = t_{hitungA} + t_{routing} + t_{kirimA} + t_{hitungB} + t_{kirimB} + t_{hitungK} + t_{kirimK} + t_{hitungK'} + t_{kirimK'} + t_{approval} \tag{7}$$

Sedangkan persamaan untuk menghitung energi yang dikeluarkan selama proses authentikasi didapatkan dari persamaan (6).

V. IMPLEMENTASI DAN ANALISIS

Proses komunikasi yang terdapat pada system di gambar 1 adalah sebagai berikut :

a. Authentikasi:
   Node dan server saling berkomunikasi secara *ad-hoc* untuk mempertukarkan kunci simetris menggunakan metode Diffie-Hellman
b. Kirim data kWh
   Data berupa penggunaan listrik di setiap rumah akan dikirimkan oleh setiap node ke server untuk pengolahan lebih lanjut. Hanya node yang ter-authentikasi saja yang dapat mengirimkan data kWh. Kunci yang dihasilkan dari proses authentikasi menjadi masukan untuk proses enkripsi data kWh menggunakan algoritma RSA.
c. Refresh Kunci
   Untuk menghindari penyusup yang mencoba mengubah data, maka kunci selalu di *refresh* secara periodik, dengan nilai seperti yang terlihat pada tabel 1.

1 Skenario Pengujian

Proses komunikasi di awali dengan pencarian rute terpendek menggunakan protokol ruting AODV antara node (1,1) dengan server di koordinat (4,8) seperti yang terlihat pada gambar 2. Proses berikutnya adalah *handshaking* antara node

dan server yang dilakukan dengan cara menukarkan kunci simetris Diffie-Hellman yang berguna untuk proses authentikasi. Panjang kunci yang digunakan untuk proses authentikasi bervariasi dari 128, 256, 512, dan 1024 bit. Simulasi dilakukan dengan 2 cara, yaitu dengan kegagalan link dan tanpa kegagalan link pada saat menggunakan protokol AODV.

2 Hasil Pengujian

2.1 Waktu Proses

Hasil simulasi dengan dengan panjang kunci yang berbeda-beda menghasilkan waktu proses authentikasi yang berbanding lurus dengan panjang kunci tersebut. Detail dari hasil simulasi dapat dilihat pada Tabel 2. Waktu total merupakan waktu yang dibutuhkan sensor untuk melakukan proses authentikasi dan enkripsi data. Sedangkan waktu total_*brokenlink* merupakan waktu total saat link putus dalam proses ruting sehingga perlu dicari rute lain, ditambah dengan waktu enkripsi. Tampak dari hasil simulasi di tabel 2 bahwa kisaran waktu yang diperlukan node untuk mencari rute ulang dikarenakan link yang putus berada di kisaran nilai 0.5 detik.

Tabel 2. Waktu Authentikasi dan Enkripsi di Sensor

Panjang Kunci (bit)	t_{auth} (s)	$t_{auth\_brokenlink}$ (s)	t_{enkrip} (s)	t_{total} (s)	$t_{total\_brokenlink}$ (s)
128	5.611	6.095	5.632	11.243	11.726
256	5.988	6.503	5.710	11.698	12.213
512	6.638	7.192	5.725	12.363	12.917
1024	7.444	8.349	5.928	13.372	14.277

2.2 Penggunaan Energi untuk Authentikasi dan Enkripsi

Energi yang dikeluarkan oleh node selama proses authentikasi baik saat link putus maupun tidak dapat dilihat pada Tabel 3. Dari tabel tersebut tampak pula jumlah energi total untuk authentikasi dan enkripsi. Perbedaan total energi yang dikeluarkan saat link putus tidak terlalu signifikan dibandingkan dengan saat link hidup, yaitu kurang dari 50 mJ.

Tabel 3. Penggunaan Energi untuk Authentikasi dan Enkripsi di Sensor

Panjang Kunci (bit)	E_{auth} (J)	$E_{auth\_brokenlink}$ (J)	E_{enkrip} (J)	E_{total} (J)	$E_{total\_brokenlink}$ (J)
128	0.286	0.311	0.287	0.573	0.598
256	0.305	0.332	0.291	0.597	0.623
512	0.339	0.367	0.292	0.631	0.659
1024	0.380	0.426	0.302	0.682	0.728

Dengan pertimbangan besar waktu proses dan total konsumsi energi untuk authentikasi dan enkripsi seperti yang tercantum pada Tabel 2 dan Tabel 3, maka dapat disimpulkan bahwa proses authentikasi akan menjadi optimal untuk panjang kunci 1024 dengan periode *refreshment* kunci per 24 jam sekali. Hal ini disebabkan total waktu dan total energi yang dibutuhkan oleh kunci sepanjang 1024 bit selama 24 jam lebih kecil dibandingkan dengan total waktu dan total energi yang dibutuhkan kunci sepanjang 128 bit untuk periode waktu yang sama.

Dari sisi keamanan, panjang kunci 1024 membutuhkan waktu lebih lama untuk diretas dibandingkan dengan panjang kunci 128 bit. Semakin panjang kunci, dapat diartikan semakin aman sistem yang disimulasikan.

VI. Kesimpulan dan Saran

Penggunaan distribusi kunci dan enkripsi merupakan salah satu cara untuk menerapkan aspek *privacy* di lingkungan AMR. Dalam paper ini telah disimulasikan penggunaan algoritma Diffie-Hellman untuk distribusi kunci dan algoritma RSA untuk proses enkripsi dalam pengiriman data listrik kWh diperumahan. Hasil percobaan menunjukkan bahwa periode waktu refreshment kunci mempengaruhi total energi dan waktu proses yang dibutuhkan untuk authentikasi dan enkripsi. Sementara panjang kunci tidak terlalu berpengaruh terhadap besar energi dan total waktu proses. Panjang kunci lebih berpengaruh terhadap aspek *privacy*, dimana semakin panjang kunci maka semakin lama waktu yang diperlukan untuk meretasnya, dan system dianggap lebih aman. Pengembangan lebih lanjut dapat dilakukan dengan menerapkan algoritma distribusi kunci maupun enkripsi yang lebih sederhana namun cukup aman. Selain itu, pemodelan *privacy* di lingkungan AMR dengan metode yang berbeda dapat menjadi alternatif solusi untuk menerapkan aspek *privacy*.

Referensi

[1] George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair. Distributed System : Concept and Design. 5th ed. Addison Wesley. 2013.

[2] The Internet of Things draft IETF : http://tools.ietf.org/html/draft-lee-iot-problem-statement-05]. 2013.

[3] SANS Institute, *Securing the Internet of Things Survey*. Januari 2014.

[4] J. Sathish Kumar, Dhiren R. Patel. A Survey on Internet of Things: Security and Privacy Issue. Internasional Journal of Computer Applications vol. 90 no.11, March 2014

[5] Tobias Heer, Oscar Garcia-Morchon, Rene Hummen, Sye Loong Keoh, Sandeep S. Kumar, and Klaus Wehrle. Security Challenges in the IP-based Internet of Things. Wireless Personal Communications Journal. December 2011, Volume 61, Issue 3, pp 527-542.

[6] Dr. Ovidiu Vermesan, Dr. Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Dr. Alessandro Bassi, Ignacio Soler Jubert, Dr. Margaretha Mazura, Dr. Mark Harrison, Dr. Markus Eisenhauer, Dr. Pat Doody. *Internet of Things Strategic Research Roadmap*. 2011.

[7] Sasa Radomirovic. *Towards a Model for Security and Privacy in the Internet of Things*. 1st International Workshop on the Security of the Internet of Things, 2010.

[8] DU Jiang, CHAO ShiWei. A Study of Information Security for M2M of lOT. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010.

[9] Antonio J. Jara, Latif Ladid, Antonio Skarmeta. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Internasional Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 3, pp. 97-118

[10] Dorice Nyamy, Pascal Urien. HIP-TAG, a New Paradigm for the Internet of Things. 1st International IEEE Workshop on Emerging Densely Connected Networks (EDCN). 2011.

[11] IEEE Standard 1888.3™-2013 or IEEE Standard for Ubiquitous Green Community Control Network: Security.

[12] European Union. IoT Privacy, Data Protection, Information Security. January 2013.

[13] Internet security glossary (RFC 2828)

[14] Luigi Atzori, Antonio Iera, Giacomo Morabito. The Internet of Things: A Survey. The International Journal Of Computer and Telecommunications Networking. 2010.

[15] Selo Sulistyo, Shaga Shaulagara, I Nyoman Yuliarsa. Rancang Bangun Jaringan Sensor Nirkabel untuk Memonitor Pemakaian Energi Listrik Pelanggan Rumah Tangga. Laporan Akhir Penelitian Unggulan Perguruan Tinggi. 2013.

[16] Ariel Bleicher. Article pada IEEE Spectrum : Privacy on the Smart Grid. 5 Oktober 2010. http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid

[17] RFC 2631 : Diffie-Hellman Key Agreement Method.

[18] Memsic Technology Inc., "IRIS XM2110CA Data Sheet." Online : http://www.memsic.com.

[19] http://www.usclcorp.com/news/amr.htm