Studi Literatur: Analisis Privasi Pada Internet of Things

Suparman
Universitas Esa Unggul
Jalan Arjuna Utara No.9, Kebon Jeruk, Jakarta 11510
e-mail: arman2307@gmail.com

Abstrak

Abstract— Potensi ancaman terhadap privasi terkait dengan lingkungan Internet of Things menjadi sebuah perhatian yang harus diperhatikan dan diberikan perlindungan mengingat data atau informasi tersebut bisa disalahgunakan untuk kepentingan yang tidak dapat dipertangungjawabkan. Tulisan ini menjelaskan dan melaporkan secara sistematis tinjauan literatur mengenai teknologi dan motode yang digunakan dalam melindungi privasi serta menganalisis solusi yang digunakan. Kami menemukan sangat sedikit yang memenuhi solusi untuk melindungi privasi tersebut dan secara khusus kami menemukan sebagian besar asumsi kesadaran pengguna dalam menjaga privasi mereka, sehingga bisa menjadi topik penelitian berikutnya untuk mengetahui keterkaitan metode dalam melindungi privasi terhadap prilaku kesadaran pengguna.

Kata kunci: *Internet of Things, IoT, Privacy*

1. Pendahuluan

Internet of Things (IoT) adalah hal yang baru, namun sekaligus merupakan istilah lama. Hal itu sudah disebutkan oleh Kevin Ashton pada tahun 1999. Mendefinisikan istilah IoT mungkin agak sulit karena memiliki banyak definisi tergantung pada siapa yang mendefinisikan istilah tersebut. Konsep dasar IoT adalah menghubungkan benda-benda atau perangkat elektronik bersama-sama, sehingga memungkinkan saling berkomunikasi satu sama lain dan memungkinkan orang berkomunikasi dengan peralatan tersebut [15]. Tren *Internet of Things* (IoT) terus tumbuh, seiring makin banyaknya perusahaan besar dan kecil yang berlomba-lomba mengkoneksikan segala macam perangkat, perlengkapan rumah tangga, bahkan mobil dan teknologi lainnya, antar sesama dengan Internet. Adopsi IoT telah merambah hampir di semua lini kehidupan. Contoh nyatanya pun semakin terlihat dengan banyaknya perangkat-perangkat terkoneksi yang tersebar dan digunakan oleh banyak orang di dunia, tak terkecuali di Indonesia. Hal ini terjadi seiring dengan peningkatan konektivitas jaringan internet.

Mengaitkan dunia fisik dengan dunia maya dan menerapkan konsep tersebut untuk semua hal membuka kemungkinan baru dalam teknologi informasi dalam arti dapat setiap saat mengakses sesuatu dari manapun. Menyediakan kemungkinan baru dalam teknologi informasi juga akan menimbulkan ancaman baru, risiko keamanan, dan kerentanan yang terbuka dalam dunia yang belum terjamah untuk saling berhubungan. Interkonektivitas adalah karakteristik dasar untuk IoT karena keseluruhan konsep dibangun di atas gagasan tersebut untuk dapat menghubungkan. Tantangan terbesar IoT adalah heterogenitas karena ada banyaknya protokol yang berbeda yang digunakan. Berinteraksi dengan beberapa perangkat melalui beberapa jaringan akan menantang baik dari sisi keamanan maupun teknis, dikarenakan protokolnya mungkin berbeda, tergantung pada apakah perangkat berkomunikasi melalui satu antarmuka (*interface*) atau antarmuka lain (misalnya, WAN Selular (3G/4G), Ethernet, atau Wi-Fi). Oleh karena itu, ada beberapa persyaratan yang relevan untuk IoT, seperti keamanan dan perlindungan privasi. Jika semuanya terhubung, maka banyak ancaman keamanan akan timbul yang menyebabkan kerahasiaan, integritas, ketersediaan, dan keaslian menjadi lebih penting terutama karena akan ada lebih banyak data dan layanan (*service*) yang tersedia dan karena semakin banyak kegiatan akan bergantung pada informasi tersebut.

Penggunaan IoT memberikan kenyaman namun hal tersebut tidak menutup kemungkinan menimbulkan masalah privasi berkenaan dengan pengunaan tersebut [1]. Keamanan juga mencakup pertimbangan privasi, karena data yang dikumpulkan misalnya sensor mungkin berisi informasi yang sensitif informasi pribadi seseorang seperti data kesehatan, lokasi, video dan data lainnya yang diambil dari perangkat yang digunakan. Integritas harus dipertimbangkan di semua tahap mulai dari penginderaan, penyimpanan, transmisi, akses dan lainnya yang berarti keamanan dan privasi di dalam IoT harus

disesuaikan dengan berbagai perangkat dan jaringan. Pada kenyataannya bahwa penyedia layanan perlu mengakses informasi tertentu untuk memberikan layanan yang sesuai, namun hal tersebut informasi yang ada dapat dilindungi dan tidak dibagi terhadap pihak lain [26].

Kontribusi makalah ini adalah untuk memberikan gambaran umum mengenai penelitian terkait privasi IoT yang ada untuk mengidentifikasi area fokus dan untuk menyoroti area yang layak mendapat perhatian lebih. Tinjauan literatur ini bertujuan untuk mengidentifikasi dan menganalisis kecenderungan penelitian, kumpulan data, metode dan kerangka kerja yang digunakan, teknologi dan aplikasi yang digunakan, ancaman dan motede perlindungan privasi. Makalah ini disusun sebagai berikut; Bagian 1 dan 2 menjelaskan latarbelakang dan penjelasan sedangkan pada bagian 3, menjelaskan metodelogi penelitian yang digunakan. Hasil dan jawaban pertanyaan penelitian disajikan pada bagian 4. Akhirnya, makalah ini dirangkum dalam bagian terakhir

2. Privasi
2.1. Definisi

Privasi merupakan tingkatan interaksi atau keterbukaan yang dikehendaki seseorang pada suatu kondisi atau situasi tertentu. Tingkatan privasi yang diinginkan itu menyangkut keterbukaan atau ketertutupan, yaitu adanya keinginan untuk berinteraksi dengan orang lain, atau justru ingin menghindar atau berusaha supaya sukar dicapai oleh orang lain. Adapun definisi lain dari privasi yaitu sebagai suatu kemampuan untuk mengontrol interaksi, kemampuan untuk memperoleh pilihan atau kemampuan untuk mencapai interaksi seperti yang diinginkan.

Privasi mempunyai konsep multi dimensi yang terkait dengan empat komponen yaitu tubuh, komunikasi, wilayah, dan informasi. Privasi tubuh berfokus pada perlindungan fisik sesorang terhadap apapun. Privasi komunikasi berfokus pada perlindungan informasi yang dilakukan melalui media apapun antara dua belah pihak seperti layanan email, telepon, dan informasi lainnya yang diberikan kepada penyedia layanan. Privasi wilayah adalah tentang menetapkan batasan wilayah, ruang fisik atau properti seperti rumah, tempat kerja dan tempat umum. Sedangkan privasi informasi mengacu pada data pribadi dikumpulkan dan diproses oleh organisasi tertentu seperti catatan layanan kesehatan dan informasi perbankan [15].

2.2. Ancaman Terhadap Privasi

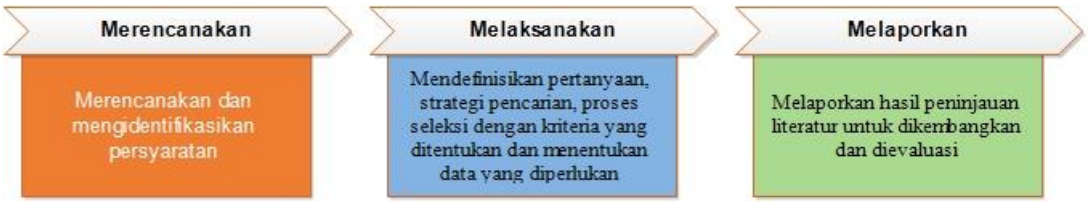
Pada era kemajuan teknologi IoT yang sangat berkembang pesat saat ini, semakin sulit kita untuk mempertahankan data privasi, hal tersebut banyaknya perangkat IoT yang mengambil alih kehidupan kita sehari-hari. Ziegeldorf [26] telah menjelaskan secara umum mengenai ancaman privasi ini yaitu:

1. Identifikasi, hal ini adalah menjadi domain ancaman secara umum seperti penyalahgunaan informasi mengenai nama dan alamat seseorang.
2. Lokasi, merupakan ancaman untuk menemukan lokasi seseorang melalui cara yang berbeda seperti GPS, lalu lintas internet dan ponsel pintar.
3. Profil, Sebagian besar digunakan untuk personalisasi dalam media seperti iklan atau lainnya yang mengatasnamakan seseorang
4. Interaksi dan presentasi, hal ini mengacu pada perangkat cerdas yang dapat berinteraksi terhadap penggunanya dapat menjadi ancaman saat data pribadi tersebut dipertukarkan antara sistem atau pengguna lain.
5. *Life cycle* IoT, atau siklus hidup dari perangkat IoT yang telah dijual atau digunakan orang lain yang masih menyimpan data atau informasi pengguna awal yang belum dihapus, hal ini menjadi ancaman yang serius.
6. Serangan inventori yaitu serangan yang dilakukan untuk akses tidak sah dan menunggu waktu yang aman untuk melakukan serangan.

3. Metode Penelitian
3.1. Metode Literatur

Penelitian ini mengunakan pendekatan sistemastis untuk meninjau literatur mengenai analisis privasi dalam *internet of things*. *Systematic literature review* (SLR) atau disebut tinjauan pustaka sistematis adalah metode yang mengidentifikasi, menilai, menginterpretasi seluruh temuan-temuan pada suatu topik penelitian, dan untuk menjawab pertanyaan penelitian (*research question*) yang telah ditetapkan sebelumnya [27].

Seperti ditunjukan pada Gambar 1. SLR dilakukan dalam tiga tahap yaitu merencanakam, melaksanakan dan dan melaporkan tinjauan literatur tersebut. Pada langkah pertama yaitu mengidentifikasikan persyaratan dengan melakukan peninjauan literatur mengenai privasi pada internet of things dan merencanakan hal-hal yang diperlukan untuk mengurangi bias dalam penelitian. Langkah kedua yaitu mendefinisikan pertanyaan penelitian, strategi pencarian, proses seleksi dengan kriteria yang ditentukan dan menentukan data yang diperlukan. Tahap terakhir yaitu melaporkan hasil peninjauan literatur untuk dikembangkan dan dievaluasi.



Gambar 1. Tahapan SLR

3.2 Pertanyaan Penelitian

Pertanyaan penelitian atau *research question* (RQ) ditentukan untuk menjaga agar tinjauan literatur tetap fokus terhadap penelitaian yang diinginkan dan digunakan untuk menuntun proses pencarian dan ekstraksi literatur. Analisis dan sintesis data, sebagai hasil dari SLR, adalah jawaban dari RQ yang kita tentukan di depan. RQ yang baik adalah yang bermanfaat, terukur, arahnya ke pemahaman terhadap topik penelitian.

Pertanyaan dan motivasi penelitian mengenai analisis privasi pada internet of things ditunjukan pada tabel 1.

Tabel 1. Pertanyaan Penelitian

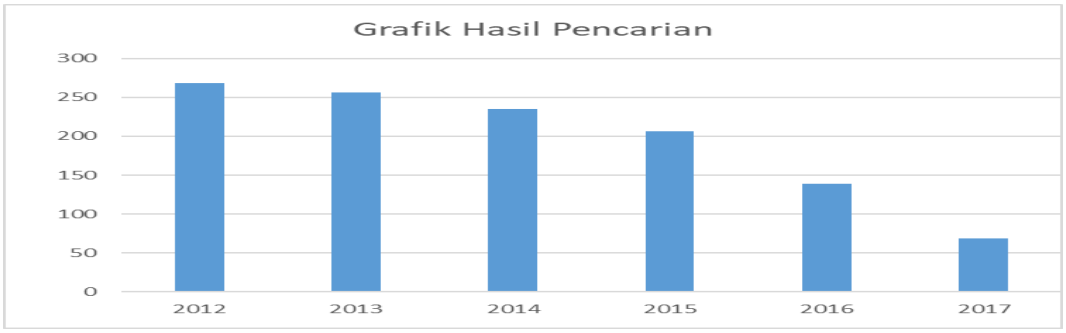
ID	Pertanyaan Penelitian	Motivasi Penelitian
1	Jurnal mana yang paling signifikan menerangkan privasi pada IoT	Untuk mengetahui jurnal yang mana yang secara kredibilitas dalam penelitian tersebut
2	Teknlogi apa yang digunakan untuk IoT yang terkait dengan privasi	Untuk memberikan informasi teknologi apa yang digunakan dalam IoT terkait dengan layanan privasi
3	Metode atau teknik apa yang digunakan untuk melindugi privasi dalam IoT	Mengetahui teknik atau metode apa yang digunakan dalam melindugi privasi dalam lingkungan IoT

3.3 Batasan Penelitian

Pembatasan penelitian dilakukan untuk menetukan fokus dan tidak meluas pada pembahasan yang dimaksud. Pembatasan tersebut meliputi tahun penerbitan yaitu dari tahun 2012 hingga tahun 2017, Jurnal yang dipublikasikan merupakan jurnal international, fokus pencarian terhadap privasi individu namun dalam beberapa kasus mungkin akan sulit untuk membedakan dengan lingkup kemanan dengan keyword atau kata kunci pencarian yaitu '*internet of things'*, 'IoT' dan dikombinasikan dengan '*Privacy*'. Batasan terakhir yaitu penelitian yang ada telah diimplementasikan atau sudah diuji coba.

4. Hasil Analisa Penelitian

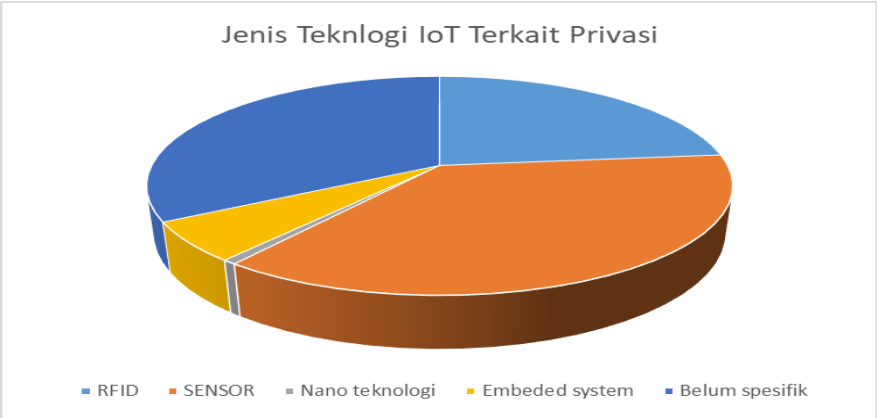
Pencarian jurnal dilakukan dengan mengunakan Google Scholar. Berikut ini terlihat pada Gambar 2. adalah data hasil pencarian dengan mengunakan Google Scholar dengan kata kunci yaitu "*privacy Internet of Things*"



Gambar 2. Penelitian Privasi Internet of Things dalam pertahun

Dari hasil pencarian data tersebut didapatkan sebanyak 83 jurnal namun dengan adanya pembatasan penelitian dan pertanyaan penelitian agar fokus terhadap pembahasan sehingga mendapatkan literatur yang dipilih menjadi 26. Hal ini menjawab pertanyaan pertama (RQ1) mengenai jurnal yang signifikan dalam penelitian.

Hasil penelitian yang didapat bahwa jenis teknologi atau perangkat yang digunakan sebagian besar terdiri dari RFID, sensor, nano teknlogi, *embeded system*, dan perangkat yang belum spesifik. Persentase jumlah perangkat tersebut dapat dilihat pada Gambar 3. Berikut ini dan sekaligus dapat menjawab pertanyaan kedua (RQ2) dalam penelitian ini.



Gambar 3. Perangkat IoT

Metode yang digunakan oleh berbagai peneliti dirangkum dalam lima kategori metode yang digunakan yaitu teknik manipulasi informasi atau kriptografi (*Cryptographic techniques- information manipulation*), minimalisasi data (*data minimization*), pembatasan akses (*access control*), Kesadaran akan privasi (*Privacy awareness*), dan lainnya. Seperti pada Table 2. berikut ini dapat menjelaskan dan memetakan jumlah metode perlindungan terhadap privasi yang digunakan oleh berbagai peneliti yang sudah diimplementasikan dan menjawab pertanyaan penelitian ketiga (RQ3).

Tabel 2. Metode Perlindungan Privasi

No	Metode Perlindungan Privasi	Total	Referensi literatur
1	Teknik manipulasi informasi atau kriptografi (*Cryptographic*)	14	[1, 2, 3, 4, 5, 7, 8, 9, 10,11, 12, 13, 14, 15]
2	Minimalisasi data (*data minimization*)	3	[16, 17, 18]
3	Pembatasan akses (*access control*)	3	[1, 19, 14]
4	Kesadaran akan privasi *(Privacy awareness*)	12	[1, 19, 21, 9, 22, 17, 23, 24, 13, 25, 18, 26]
5	Lainnya	2	[24, 25]

5. Diskusi

Hasil studi literatur tersebut telah menyajikan tentang apa dan bagaimana penelitian mengenai privasi terkait dengan lingkungan IoT sehingga memungkinkan untuk mengidentifikasikan kesenjagan antara berbagai penelitian yan telah dilakukan sebelumnya.

Terlihat pada hasil pembahasan bahwa pencarian literatur dengan menggunakan Google Scholar dengan kata kunci yang telah ditentukan terlihat bahwa penelitian mengenai privasi yang terkait dengan perangkat IoT selama 6 tahun ini mengalami kecenderungan menurun hal ini menjadikan pertanyaan apakah penelitian privasi dalam hal ini terkait dengan IoT bukan menjadi pokok permasalahan yang berarti atau permasalahan tersebut sudah terselesaikan.

Disisi lain kita melihat bahwa teknologi yang digunakan dalam lingkungan IoT kecenderungan terbesar yang digunakan yaitu sensor. Sedangkan pada metode perlindungan privasi yang banyak digunakan yaitu dengan manipulasi informasi atau dengan teknik kriptografi. Sehubungan dengan hal tersebut, kita bisa mengambil sebuah pertanyaan apakah saat ini teknologi sensor yang digunakan sudah mampu untuk memanipulasi informasi yang dikirimkan ke sebuah layanan untuk melindungi informasi tersebut atau dengan cara menggunkan metode lainnya.

Kesadaran akan privasi banyak juga dibahas oleh peneliti sebelumnya. Hal ini mengindikasikan bahwa kesadaran akan diri sendiri terhadap privasi ini sangat diperlukan sebagai langkah awal dalam melindungi informasi yang menyangkut privasi pengguna. Hal tersebut juga perlu dilakukan oleh para pemberi layanan untuk diinfomasikan kepada pengguna untuk menjamin dan memberikan kepastian akan perlindungan informasi atau data privasi yang diberikan pengguna terhadap pemberi layanan atau organisasi yang terlibat.

5. Kesimpulan

Memasuki era *Internet of things* setiap elemen masyarakat mau tidak mau harus bersiap untuk mengikuti tren teknologi terbaru tersebut. Dengan semakin terkoneksinya sesuatu yang bisa menghubungkan data dengan produk lain muncul isu keamanan dan privasi. Hal ini tentu saja sesuatu yang lumrah karena data akan terkait dengan bagaimana data tersebut dilindungi dan tentang siapa data dan siapa saja yang bisa melihat data tersebut.

Internet of Things ini seolah-olah sebuah panggung sandiwara privasi baru di mana penonton diundang untuk berbagi informasi dengan menggunakan smartphone atau perangkat lain mereka yang menyebabkan data tentang pribadi mereka tetap hidup dan tanpa sadar meninggalkan jejak digital. Kekhawatiran lain terkait masalah privasi ini adalah produsen yang bertindak tergesa-gesa untuk merilis produk mereka ke pasar secepat mungkin, namun karena tidak memperhatikan privasi dan keamanan akhirnya malah harus membayar harga atas perilisan yang tergesa-gesa tersebut.

Masalah privasi saat ini masih sering terjadi pelanggaran oleh sebab itu diperlukannya penelitian lanjutan mengenai metode paling tepat untuk melindungi privasi pengguna atau informasi perangkat dalam lingkungan aplikasi yang berbeda sehingga nantinya dapat memberikan referensi ilmiah untuk menyelesaikan permasalahan privasi tersebut.

Daftar Pustaka

[1] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru. *A reference architecture for improving security and privacy in internet of things applications. In Mobile Services (MS)*, 2014 IEEE International Conference on, pages 108–115. IEEE, 2014

[2] W. Tan, K. Xu, and D. Wang. *An anti-tracking source-location privacy protection protocol in wsns based on path extension. Internet of Things Journal*, IEEE, 1(5):461–471, 2014.

[3] I. Nakagawa, Y. Hashimoto, M. Goto, M. Hiji, Y. Kicuchi, M. Fukumoto, and S. Shimojo. *Dht extension of m-cloud–scalable and distributed privacy preserving statistical computation on public cloud. In Computer Software and Applications Conference (COMPSAC)*, 2015 IEEE 39th Annual, volume 3, pages 682–683. IEEE, 2015.

[4] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen. Cpal: *A conditional privacy-preserving authentication with access linkability for roaming service. Internet of Things Journal*, IEEE, 1(1):46–57, 2014.

[5] M. Florian, S. Finster, and I. Baumgart. *Privacy-preserving cooperative route planning*. Internet of Things Journal, IEEE, 1(6):590–599, 2014.

[6] H. C. Pohls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. Diaz Rodriguez, and T. Mouroutis. Rerum: *Building a reliable iot upon privacy-and security-enabled smart objects*. In Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE, pages 122–127. IEEE, 2014.

[7] S. N. Premnath and Z. J. Haas. *Security and privacy in the internetof-things under time-and-budget-limited adversary model*. Wireless Communications Letters, IEEE, 4(3):277–280, 2015.

[8] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang. *A medical healthcare system for privacy protection based on iot. In Parallel Architectures, Algorithms and Programming (PAAP)*, 2015 Seventh International Symposium on, pages 217–222. IEEE, 2015.

[9] D. Banerjee, B. Dong, M. Taghizadeh, and S. Biswas. *Privacy-preserving channel access for internet of things*. Internet of Things Journal, IEEE, 1(5):430–445, 2014.

[10] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. *Network-level security and privacy control for smarthome iot devices. In Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015 IEEE 11th International Conference on, pages 163–167. IEEE, 2015

[11] T. Bose, S. Bandyopadhyay, A. Ukil, A. Bhattacharyya, and A. Pal. *Why not keep your personal data secure yet private in iot?: Our lightweight approach. In Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2015 IEEE Tenth International Conference on, pages 1–6. IEEE, 2015.

[12] K.-S. Wong and M. H. Kim. *Towards self-awareness privacy protection for internet of things data collection*. Journal of Applied Mathematics, 2014.

[13] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. Moreno. *A decentralized approach for security and privacy challenges in the internet of things. In Internet of Things (WF-IoT)*, 2014 IEEE World Forum on, pages 67–72. IEEE, 2014.

[14] X. Wang, J. Zhang, E. M. Schooler, and M. Ion. *Performance evaluation of attribute-based encryption: Toward data privacy in the iot. In Communications (ICC)*, 2014 IEEE International Conference on, pages 725–730. IEEE, 2014.

[15] M. Enev. *Machine Learning based Attacks and Defenses in Computer Security: Towards Privacy and Utility Balance in Emerging Technology Environments*. PhD thesis, University of Washington, Seattle, WA, August, 2014.

[16] T. Bose, S. Bandyopadhyay, A. Ukil, A. Bhattacharyya, and A. Pal. *Why not keep your personal data secure yet private in iot?: Our lightweight approach. In Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2015 IEEE Tenth International Conference on, pages 1–6. IEEE, 2015.

[17] A. Samani, H. H. Ghenniwa, and A. Wahaishi. *Privacy in internet of things: A model and protection framework*. Procedia Computer Science, 52:606–613, 2015.

[18] A. Huertas Celdran, G. Clemente, J. Felix, M. Gil Perez, and G. Martinez Perez. *Secoman: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications*. IEEE Systems Journal, 99:1–14, 2013.

[19] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. *Network-level security and privacy control for smarthome iot devices. In Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015 IEEE 11th International Conference on, pages 163–167. IEEE, 2015.

[20] Y. Yao, L. T. Yang, and N. N. Xiong. *Anonymity-based privacypreserving data reporting for participatory sensing*. IEEE Internet of Things Journal, 2(5):381–390, 2015.

[21] A. Ukil, S. Bandyopadhyay, and A. Pal. *Sensitivity inspector: Detecting privacy in smart energy applications. In Computers and Communication (ISCC)*, 2014 IEEE Symposium on, pages 1–6. IEEE, 2014.

[22] A. Ukil, S. Bandyopadhyay, and A. Pal. *Privacy for iot: Involuntary privacy enablement for smart energy systems*. In Communications (ICC), 2015 IEEE International Conference on, pages 536–541. IEEE, 2015.

[23] A. Ukil, S. Bandyopadhyay, and A. Pal. *Iot-privacy: To be private or not to be private. In Computer Communications Workshops (INFOCOM WKSHPS)*, 2014 IEEE Conference on, pages 123–124. IEEE, 2014.

[24] C. Kang, F. Abbas, and H. Oh. *Protection scheme for iot devices using introspection. In Network of the Future (NOF)*, 2015 6th International Conference on the, pages 1–5. IEEE, 2015.

[25] Y. Liu, X. Gong, and C. Xing. *A novel trust-based secure data aggregation for internet of things*. In Computer Science & Education (ICCSE), 2014 9th International Conference on, pages 435–439. IEEE, 2014.

[26] A. Arabo. *Privacy-aware iot cloud survivability for future connected home ecosystem. In Computer Systems and Applications (AICCSA)*, 2014 IEEE/ACS 11th International Conference on, pages 803–809. IEEE, 2014.

[27] Romi Satria Wahono. *A Systematic Literature Review of Software Defect Prediction: Research Trends, Datasets, Methods and Frameworks*, Journal of Software Engineering, Vol. 1, No. 1, 2015.

[28] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle. *Privacy in the internet of things: threats and challenges*. Security and Communication Networks, 7(12):2728–2742, 2014.