JURNAL ILMU TEKNIK DAN INFORMATIKA (TEKNIK) VOL 3, No.1, Mei 2023, pp. 35 - 54
p-ISSN : 2808-8751 (print)
e-ISSN : 2798-2513 (online)
http://journal.stiestekom.ac.id/index.php/TEKNIK · page 34

User Interface Berbasis Web Pada Perangkat Internet Of Things

Sigit Umar Anggono[1], Edy Siswanto[2], Laksamana Rajendra Haidar Azani Fajri[3], Munifah[4]
[1]Universitas Sains dan Teknologi Komputer Semarang
Jl. Majapahit 605 Semarang, e-mail: sigit@gmail.com
[2]Universitas Sains dan Teknologi Komputer Semarang
Jl. Majapahit 605 Semarang, e-mail: edy@stekom.ac.id
[3]Universitas Sains dan Teknologi Komputer Semarang
Jl. Majapahit 605 Semarang, e-mail: laksamanahaidar@stekom.ac.id
[4]Universitas Sains dan Teknologi Komputer Semarang
Jl. Majapahit 605 Semarang, e-mail: munifah@stekom.ac.id

ARTICLE INFO

Article history:

Received maret 2023
Received in revised form
Accepted April 2023
Available online Mei 2023

ABSTRAK

Tujuan Utama: Tujuan utama dari penelitian ini adalah untuk menyediakan User-Interface (UI) berbasis web yang dapat mengatasi tantangan dan memberikan kontrol data secara real-time. Oleh karena itu, kami telah membuat prototipe User Interface yang dapat mendemonstrasikan konsep situs web pengelola IoT dan memberikan bukti penerapan konsep tersebut. Platform yang diusulkan dimaksudkan untuk berkontribusi dalam meningkatkan persepsi pengguna terhadap perangkat IoT. Background problem: Dengan kemajuan yang berkembang dalam teknologi Internet of Things (IoT), yang menggabungkan berbagai perangkat dengan fungsi, kemampuan, dan protokol komunikasi yang berbeda, penting untuk menyediakan platform yang memungkinkan pengguna IoT untuk berinteraksi dengan perangkat IoT mereka secara langsung dan dapat kelola mereka dengan mudah melalui platform itu dari berbagai lokasi kapan saja untuk melindungi privasi mereka saat menggunakan perangkat IoT. Metode Penelitian: Metode eksperimental dan survei digunakan dalam penelitian ini untuk mengevaluasi persepsi pengguna terhadap penggunaan sebuah platform yang menggabungkan semua perangkat IoT mereka dan memungkinkan mereka mengelola perangkat berdasarkan preferensi mereka melalui platform tersebut dan melindungi privasi mereka. Temuan: Temuan menunjukkan perlunya membuat platform di mana pengguna dapat mengontrol berbagai perangkat IoT dari jarak jauh. Ini juga menunjukkan bahwa prototipe situs web adalah platform yang mudah digunakan, dan dapat digunakan dengan mudah tanpa pengalaman teknis apa pun. Pengguna dapat mengakses informasi tentang perangkat IoT yang terhubung serta mengontrolnya. Kesimpulan: Prototipe dapat digunakan untuk mendemonstrasikan konsep

Received, 2023; Revised, 2023; Accepted, 2023

p-ISSN : 2808-8751 e-ISSN : 2798-2513

aplikasi web yang diusulkan, sementara hasil survei menunjukkan kebutuhan untuk platform yang mudah digunakan untuk mengontrol perangkat IoT dari jarak jauh dan meningkatkan persepsi privasi pengguna di lingkungan IoT.

Kata Kunci: *Internet of Things, Web-based User Interface, Web Prototype, Multi-Platform*

.

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) yang pesat telah menghasilkan revolusi di berbagai bidang. Namun, terdapat banyak perangkat IoT yang tidak dilengkapi dengan User-Interface (UI) seperti layar atau tombol yang memungkinkan interaksi antara pengguna dan perangkat. Oleh karena itu, diperlukan pembuatan UI yang memungkinkan pengguna dan sistem IoT untuk berinteraksi dan berkomunikasi satu sama lain. Selain itu, masalah privasi menjadi semakin kritis seiring dengan meluasnya penggunaan perangkat yang terhubung ke internet dan sensor yang dapat mengambil data tanpa persetujuan pengguna di tempat umum. Menurut Perez et al., (2017), masalahnya adalah pihak ketiga belum memberikan izin untuk menjadi bagian dari pendataan di area publik. Sebenarnya, potensi pelanggaran privasi dapat terjadi di tempat-tempat yang tidak diharapkan orang untuk diawasi. Pada saat yang sama, jika mereka tahu bahwa mereka sedang diawasi, maka mereka tidak akan menganggap hal tersebut adalah pelanggaran privasi, tapi orang akan lebih cenderung berperilaku berbeda di tempat umum jika mereka tahu bahwa mereka sedang diawasi, sehingga, orang mungkin memiliki kekhawatiran tentang privasi data mereka. Karena inilah "orang kadang merasa tidak nyaman menggunakan atau memberikan data pribadi mereka kepada pihak ketiga" (Naeini et al., (2017). Pada dasarnya, orang-orang lebih peduli dengan teknik yang digunakan untuk berbagi data rahasia mereka daripada hanya berbagi data itu sendiri. Di mana sebagian besar dari mereka menganggap pelanggaran privasi terjadi ketika data mereka dibagikan untuk tujuan yang tidak pantas. Selain itu, karena proliferasi perangkat IoT dan keragaman pengumpulan dan penggunaan data oleh perangkat tersebut, persepsi orang tentang teknologi inovatif ini dapat berubah seiring waktu. Selain itu, karena pengumpulan data menjadi lebih mudah diakses, dan dapat dicapai tanpa kesadaran masyarakat sehingga banyak layanan IoT dapat dihindari oleh banyak orang karena pengumpulan dan pemrosesan data yang tidak terlihat. Dari sinilah, muncul kebutuhan mendesak untuk memahami perspektif orang yang berbeda tentang perangkat IoT yang terkait dengan masalah privasi dan menemukan solusi yang mudah dan mudah untuk menjaga privasi mereka dengan memenuhi berbagai preferensi privasi mereka di perangkat IoT, yang pada gilirannya berkontribusi pada perubahan persepsi orang.

Untuk mengatasi masalah privasi ini, interaksi pengguna dan pengendalian dalam perangkat IoT dibutuhkan, sehingga penelitian ini mengusulkan sistem (User-Interface Berbasis Web) untuk perangkat IoT yang memungkinkan pengguna IoT untuk berinteraksi dengan perangkat mereka dan juga menghubungkan dan mengelola perangkat IoT melalui antarmuka itu. Dengan demikian, persepsi privasi pengguna IoT bisa meningkat, dengan perangkat IoT yang dapat mengumpulkan dan menggunakan informasi pengguna secara transparan untuk memastikan bahwa persyaratan privasi pengguna terpenuhi. Pekerjaan yang diimplementasikan dalam penelitian ini adalah sebuah prototipe yang akan berkontribusi dalam penyampaian konsep User-Interface berbasis web bagi pengguna IoT untuk menghubungkan perangkat IoT mereka ke situs web dan kemudian mengelola perangkat yang terhubung tersebut melalui situs web tersebut

2. TINJAUAN PUSTAKA

IoT merupakan sistem yang menggabungkan perangkat, aktuator, sensor, protokol komunikasi, dan aplikasi yang secara independen dapat bertukar data dan perintah melalui jaringan untuk menyediakan layanan cerdas. Menghubungkan perangkat fisik ke internet memungkinkan pengguna untuk mendapatkan keuntungan dari setiap perangkat. Selain itu, perangkat IoT memberikan peningkatan kualitas layanan di organisasi mana pun dan meningkatkan produktivitas dengan menawarkan pelatihan tepat waktu untuk karyawan dan meningkatkan kemungkinan kerja jarak jauh, dan ini dapat meningkatkan produktivitas secara keseluruhan sekaligus mengurangi konsumsi daya secara signifikan. Gupta et al. (2015) mengusulkan sistem kontrol otomatis berbasis Ethernet yang hemat daya untuk mengendalikan perangkat listrik oleh perangkat IoT dari gedung institusional. Model ini digunakan di ruang kelas untuk mengontrol lampunya dan menghemat energi. Sistem yang diusulkan memiliki kinerja tinggi dalam meminimalkan daya komputasi. Sehingga perangkat dan aplikasi IoT dapat berkomunikasi satu sama lain untuk membuat

p-ISSN : 2808-8751 e-ISSN : 2798-2513

keputusan atas nama manusia. Praktisnya, IoT dapat menangkap data pengguna melalui sensor, mengirim, menerima, dan berbagi dalam beberapa kasus, informasi yang ditangkap dari pengguna. Tidak ada organisasi di dunia yang mengendalikan dan memiliki IoT sepenuhnya; oleh karena itu, tidak ada definisi IoT yang akurat dan konsisten. Namun, berbagai entitas dan banyak organisasi bermaksud mengklarifikasi istilah Internet of Things dan mendefinisikannya secara akurat dan jelas.

Arsitektur IoT

Struktur campuran dapat disajikan oleh IoT, ini mencakup berbagai arsitektur subsistem. Sistem IoT dibentuk oleh dua arsitektur manajemen: digerakkan oleh peristiwa dan berbasis waktu. Dalam hal ini, tanggal ditransmisikan saat sensor merasakan tindakan di lingkungan luar. Terkait arsitektur berbasis waktu dengan interval tertentu, data ditransmisikan secara terus menerus (Aleksandrovičs et al., (2016). Meskipun teknologi utama dan arsitektur yang mendasari IoT masih menjadi isu terbuka. Namun, banyak peneliti telah mengusulkan berbagai jenis arsitektur IoT. Salah satu arsitektur yang diusulkan untuk masa depan IoT menggabungkan atribut sosial adalah unit dan ubiquitous IoT (U2IoT) (Ning, (2016). Struktur IoT masa depan hadir untuk menghubungkan dunia fisik dengan dunia virtual dan dunia sosial. Unite and ubiquitous IoT (U2IoT) digunakan untuk menggabungkan dunia fisik dengan dunia maya. Ini mencakup beragam sistem; U2IoT mencakup IoT industri, IoT nasional, dan IoT global, yang menggabungkan banyak Unit IoT dengan karakteristik yang ada di mana-mana. Ada beberapa fitur signifikan dari model U2IoT, yaitu virtual, fisik, koeksistensi sosial, interkoneksi dan interaktivitas, konsistensi ruang-waktu, dan status multi-identitas (Ali et al., (2015). Komponen sistem ditentukan oleh arsitektur IoT, cara bekerja secara kolektif, dan cara pertukaran data di antara mereka

Aplikasi IoT

Sen et al., (2011) menjelaskan beberapa contoh penting aplikasi IoT dalam berbagai industri. Dalam industri penerbangan, IoT dapat digunakan untuk identifikasi produk dan elemen andal, sehingga dapat membantu meningkatkan keselamatan dan keamanan produk dan layanan. Dalam industri otomotif, sensor dan aktuator canggih dapat disediakan di berbagai jenis kendaraan untuk meningkatkan kualitas kontrol. Selain itu, smart things juga dapat digunakan untuk memantau dan melaporkan berbagai parameter, mulai dari tekanan ban hingga jarak kendaraan lain. Sedangkan dalam industri telekomunikasi, IoT dapat memanfaatkan berbagai teknologi telekomunikasi dan menciptakan layanan baru. IoT juga memiliki dampak penting pada kehidupan mandiri, dengan memberikan dukungan bagi populasi lanjut usia menggunakan sensor yang dapat dikenakan dan ambien untuk mendeteksi aktivitas kehidupan sehari-hari dan memantau interaksi sosial. Pada industri farmasi, paradigma IoT dapat memberikan label cerdas untuk obat-obatan, melacaknya melalui rantai pasokan, yang memungkinkan untuk mendeteksi produk palsu dan mencegah penipuan. Banyak keuntungan yang dapat diberikan oleh IoT dalam operasi ritel dan supply chain management (SCM), seperti tag RFID dan rak pintar yang melacak item saat ini secara real-time. Di industri manufaktur, proses produksi dan seluruh siklus hidup produk dapat dioptimalkan dan dipantau dengan menghubungkan item dengan teknologi informasi, melalui perangkat pintar yang disematkan atau penggunaan pengidentifikasi unik. Selain itu, ada juga beberapa aplikasi bervariasi lainnya, seperti industri proses, lingkungan, transportasi, pertanian, media, hiburan, asuransi, dan daur ulang. IoT memiliki potensi besar untuk pengembangan sejumlah besar aplikasi dan dapat meningkatkan kesejahteraan serta kualitas hidup warga melalui kerja sama antara platform, aplikasi, perangkat, dan layanan.

Kualitas Khusus IoT

IoT merupakan konsep yang mencakup sejumlah besar perangkat terintegrasi ke dalam jaringan lokal atau global, fisik, dan nirkabel. Dalam IoT, serangkaian perangkat dan sensor otomatis menghasilkan dan mentransmisikan sejumlah besar data secara real-time, dengan pemfilteran dan pemrosesan data yang memadai. Beberapa faktor penting yang perlu dipertimbangkan dalam sistem IoT seperti protokol jaringan yang berbeda, transmisi data yang kompleks, heterogenitas perangkat IoT, dan skalabilitas perlu diperhatikan. Protokol jaringan seperti Bluetooth, Wi-Fi, dan ZigBee merupakan alasan di balik transmisi data IoT. Selain itu, heterogenitas perangkat IoT menjadi fitur utama yang paling banyak karena terdiri dari berbagai perangkat yang dibagi ke dalam tiga tingkat utama, yaitu perangkat titik akhir, perangkat mediator, dan mesin komputasi. Skalabilitas menjadi faktor penting dalam jumlah komponen struktur IoT dalam sistem apa pun. Dalam IoT, kekuatan berasal dari kemampuannya untuk melakukan kombinasi proses yang rumit tanpa interaksi manusia secara langsung, yang memungkinkan pengambilan data secara

p-ISSN : 2808-8751 e-ISSN : 2798-2513

otomatis dan dilakukan analisis pada data terintegrasi dari berbagai sumber untuk mendapatkan informasi berharga yang diperlukan.

Teknologi IoT

IoT merupakan suatu konsep teknologi yang melibatkan beberapa perangkat cerdas yang terhubung dengan berbagai teknologi tertanam seperti Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Cloud Computing, dan Wireless Fidelity (Wi-Fi). Sistem RFID, terdiri dari transponder tag, pembaca tag, antena, dan antarmuka untuk mengidentifikasi elemen secara nirkabel menggunakan gelombang radio. WSN sebagai jaringan nirkabel yang dikonfigurasi penginderaan untuk memantau kondisi fisik dan lingkungan secara nirkabel seperti suhu, suara, getaran, dan tekanan sendiri dan tanpa infrastruktur. Cloud Computing dapat memanfaatkan IoT untuk mengkompensasi kendala teknologi dan memberikan layanan baru dalam banyak skenario kehidupan nyata. Teknologi Wi-Fi juga memiliki efek yang meningkat pada IoT, di mana persyaratan transmisi data melalui Wi-Fi berbeda dari transfer data kecil dan sesekali hingga sejumlah besar data tanpa gangguan. (Davis, 2016; Maor, 2018; Botta et al., 2014; Matin et al., 2012).

IoT merubah cara bisnis berkomunikasi, berkolaborasi, dan mengoordinasikan proses sehari-hari. IoT sangat ideal untuk operasi yang kompleks dan terdistribusi, memungkinkan memperoleh data akurat secara real-time dan memungkinkan pengambilan keputusan yang cepat. Namun, IoT juga merupakan tantangan keamanan karena data diperoleh dari berbagai jenis sensor jaringan yang dapat diproses oleh beberapa jenis jaringan. Implementasi IoT membutuhkan orang yang berkualifikasi tinggi, integrasi sistem, jaringan, dan aplikasi yang rumit. Ekosistem IoT terdiri dari perangkat, sensor, jaringan, penyimpanan cloud, dan aplikasi yang membantu organisasi meningkatkan posisi strategis mereka secara proaktif dan reaktif. Perangkat IoT digunakan di berbagai bidang, mulai dari penggunaan pribadi hingga industri dan utilitas perusahaan. Di perusahaan, perangkat IoT digunakan untuk meningkatkan efisiensi, memfasilitasi proses bisnis, mengurangi kesalahan, dan menghemat waktu. Ada banyak titik akhir nirkabel yang terhubung di perusahaan, termasuk banyak objek tempat kerja standar seperti kamera keamanan, kunci, printer, dan pemindai kantor, ruang rapat cerdas, dan banyak teknologi baru lainnya yang membantu meningkatkan produktivitas dan menghemat biaya dan waktu.

Ancaman Keamanan di IoT

Meskipun IoT telah berkembang jauh sejak diperkenalkan di dunia, berbagai ancaman tetap ada dari perspektif keamanan di IoT. Karena konstruksi dan fungsi yang berbeda dari lapisan IoT yang berbeda, ancaman keamanan juga berbeda untuk setiap lapisan. Kumar et al., (2016), menyebutkan beberapa ancaman keamanan di IoT yang diklasifikasikan secara independen untuk setiap lapisan.

Ancaman Lapisan Aplikasi - Lapisan aplikasi dalam sistem rentan terhadap ancaman keamanan, seperti serangan kode berbahaya, kerusakan aplikasi, ketidaktersediaan patch keamanan, dan peretasan smart grid. Oleh karena itu, tindakan preventif dan proaktif perlu dilakukan untuk menjaga keamanan lapisan aplikasi. *Ancaman Lapisan Persepsi* - Lapisan persepsi pada sebuah node mengandung sensor-sensor yang rentan terhadap ancaman keamanan seperti kerusakan atau pencurian data. Ancaman lainnya meliputi penyadapan atau menguping karena komunikasi nirkabel antara perangkat di lapisan persepsi dan kebisingan dalam data yang dapat menyebabkan kesalahan dalam tafsir data. Untuk meminimalkan risiko ancaman keamanan, diperlukan perlindungan yang tepat pada lapisan persepsi dalam sebuah node. *Ancaman Lapisan Jaringan* - Lapisan jaringan IoT rentan terhadap ancaman keamanan karena banyaknya data yang dibawanya. Ancaman utama meliputi autentikasi data, Serangan DoS, Serangan Gateway, Akses Tidak Sah, Serangan Penyimpanan, dan Injeksi Informasi Palsu. Penting untuk mengamankan lapisan jaringan untuk melindungi data dan memastikan operasi yang aman. *Ancaman lapisan fisik* - Lapisan fisik pada suatu perangkat rentan terhadap masalah keamanan eksternal dan memerlukan tindakan pengamanan untuk melindungi perangkat dan memastikan efisiensi baterai. Kumar et al. (2016) menunjukkan bahwa kerusakan fisik, serangan lingkungan, kehilangan daya, kegagalan perangkat keras, dan gangguan fisik pada pengontrol logika yang dapat diprogram (PLC) merupakan masalah keamanan yang umum terjadi pada physical layer. Tindakan pencegahan seperti meningkatkan daya tahan fisik perangkat, melindungi PLC dari gangguan eksternal, dan memperhatikan kondisi baterai perlu dilakukan untuk mengurangi risiko tersebut.

Keamanan IoT

p-ISSN : 2808-8751 e-ISSN : 2798-2513

Risiko keamanan selalu ada di IoT pada berbagai lapisan berbeda tergantung pada konstruksi lapisan itu. Sama seperti ancaman keamanan yang berbeda untuk setiap lapisan, skema untuk meminimalkan risiko juga terpisah untuk setiap lapisan tergantung pada risiko yang mereka hadapi. Beberapa metode perlindungan terhadap risiko keamanan yang berbeda di setiap lapisan yang diadopsi dari Kumar et al., (2016).

Keamanan Lapisan Aplikasi - Banyak skema keamanan yang telah diusulkan oleh peneliti berbeda untuk mengatasi risiko keamanan pada lapisan aplikasi. Beberapa solusi yang ditawarkan antara lain: Pendekatan Domain-Specific Metrics (DSM) yang bertujuan untuk meningkatkan metrik keamanan informasi eHealth dengan mengusulkan lima elemen terkait keamanan informasi. Teori Game, teknik matematika yang didasarkan pada pertempuran serangan keamanan oleh sistem kompleks dinamis dengan menyerang mereka untuk memastikan keamanan yang lebih baik dari lapisan aplikasi. Metrik Komprehensif dan Komparatif untuk Keamanan Informasi (CCM) yang menggunakan metrik keamanan melalui pendekatan penilaian risiko untuk meningkatkan keamanan. Adaptive Security and Trust Management (ASTM) yang merupakan fitur keamanan dinamis dengan kemampuan beradaptasi dengan perubahan lingkungan untuk mengantisipasi ancaman yang tidak diketahui, serta menggunakan pembelajaran adaptif dengan mengubah parameter internal untuk merasakan perubahan dinamis dalam sistem. (Abie et al., 2012).

Keamanan Lapisan Persepsi - Berbagai teknik telah dikembangkan untuk meningkatkan keamanan di lapisan persepsi. ASM menggunakan teknik empat langkah untuk mengidentifikasi tujuan keamanan dan beradaptasi dengan lingkungan yang berubah sesuai dengan metrik keamanan. SMC memastikan keamanan yang lebih baik dengan mengelola dan mengukur sumber daya yang memanfaatkan komputasi di mana-mana dengan kebijakan, layanan penemuan, dan peran yang ditentukan. PKI dirancang khusus untuk mengatasi ancaman keamanan pada node. Sensor Cyber memastikan akuisisi dan penggunaan data secara real-time untuk meminimalkan kemungkinan serangan data saat berada di cloud. AAL memastikan fitur keamanan yang lebih baik di IoT, terutama untuk keselamatan lansia. Semua teknik ini telah dikembangkan oleh para peneliti dengan tujuan meningkatkan keamanan di lapisan persepsi (Savola et al., 2012; Li et al., 2013; Ning et al., 2013; Dohr et al., 2010).

Keamanan Lapisan Jaringan - Ada beberapa teknik yang dapat digunakan untuk meningkatkan keamanan di lapisan jaringan IoT, yang sangat rentan terhadap risiko keamanan karena komunikasi. Solusi yang diusulkan untuk mengatasi risiko ini meliputi membuat transmisi data lebih aman. Teknik yang umum digunakan untuk tujuan ini termasuk Middleware Keamanan, Otentikasi dan Kontrol Akses, Sistem Transportasi Cerdas (ITS), dan Kerangka Manajemen Identitas. Middleware Keamanan menggunakan parameter seperti Entity Identification, Secure Storage, Security Audit, dan Enkripsi data untuk memastikan antarmuka yang aman. Otentikasi dan Kontrol Akses memastikan integritas data, sementara ITS menggunakan analisis risiko untuk memberikan metode keamanan dan meningkatkan standar kinerja yang efisien dengan mengatasi ancaman terhadap sistem transportasi. Kerangka Manajemen Identitas mengautentikasi perjalanan data antara perangkat dan penyimpanan cloud. Meskipun belum diterapkan secara praktis, teknik ini menempatkan manajer identitas dan manajer layanan pada perangkat untuk memastikan keamanan. (Liu et al., 2012; Zhao et al., 2012; Horrow et al., 2012).

Keamanan Lapisan Fisik - Lapisan fisik adalah lapisan eksternal yang terpapar lingkungan dengan perangkat di lapisan ini rentan terhadap kerusakan fisik dari pengguna serta lingkungan. Karena faktor eksternal tidak dapat dikontrol, tidak banyak teknik untuk mengatasi risiko keamanan di lapisan fisik. Skema yang paling menonjol dalam domain ini sebagai tag RFID. Ini memastikan keamanan yang lebih baik di lapisan fisik dengan memastikan semua perangkat tetap terhubung di lapisan fisik. Tag RFID ini dapat dipasang di perangkat pintar di lapisan fisik untuk memungkinkan komunikasi cepat antara perangkat yang saling terhubung dan menyelesaikan masalah identifikasi objek (Aggarwal et al., (2012).

Privasi di IoT

Perangkat IoT menghadirkan peluang luar biasa untuk kenyamanan, mereka membawa risiko privasi dengan pengaruh signifikan pada persepsi orang tentang teknologi IoT. Masalah privasi di IoT meliputi: mengontrol informasi pribadi, mengembangkan mekanisme dan peraturan privasi, dan teknik dasar untuk mengontrol pengguna identitas (Sahmim et al.., (2017). Ziegeldorf et al. (2013) membahas beberapa ancaman privasi di IoT yang harus diwaspadai oleh pengguna IoT. Ancaman privasi di IoT yang

p-ISSN : 2808-8751 e-ISSN : 2798-2513

diangkat antara lain identifikasi, pelokalan dan pelacakan, profiling, interaksi dan presentasi, transisi siklus hidup perangkat IoT, serangan inventaris, dan keterkaitan. Identifikasi menjadi masalah privasi yang serius dalam IoT. Ini akan terjadi ketika pengidentifikasi seperti alamat atau nama dapat dikaitkan dengan individu, dan kemudian data tentang individu tersebut dapat diakses. Ancaman ini dapat memicu ancaman privasi lain seperti pembuatan profil dan pelacakan. Ancaman ini bisa saja terjadi melalui teknologi sidik jari dan RFID. Ancaman lainnya adalah pelokalan dan pelacakan, yang terjadi ketika lokasi seseorang terus dipantau melalui sarana seperti GPS dan Pola Lalu Lintas Internet. Hal ini dapat menyebabkan pelanggaran privasi yang serius seperti penguntitan GPS dan pengungkapan catatan medis pribadi. Selain itu terdapat beberapa ancaman lain seperti profiling, interaksi dan presentasi, transisi siklus hidup perangkat IoT, serangan inventaris, dan keterkaitan, yang semuanya dapat memicu pelanggaran privasi yang serius jika tidak diwaspadai dengan baik. Dalam konteks IoT, masalah privasi menjadi perhatian yang serius. Kumar (2014) membahas secara luas empat kategori masalah privasi yang terjadi pada IoT. Pertama, privasi perangkat yang berkaitan dengan akses tidak sah ke perangkat dan lokasi perangkat yang dapat mengungkap lokasi dudukan perangkat. Kedua, privasi komunikasi yang terkait dengan pelacakan data saat transmisi data yang menggunakan enkripsi dan penambahan data ke paket, yang dapat membahayakan data. Ketiga, privasi inventaris yang menghadapi masalah terkait informasi pribadi yang terkait dengan identitas asli dan dapat menimbulkan risiko terhadap privasi pengguna. Terakhir, memproses privasi yang memerlukan pemrosesan data pribadi dengan cara yang mencapai tujuan yang disyaratkan dan tetap dilindungi, bahkan tanpa izin eksplisit dari pemilik data tersebut untuk diungkapkan. Oleh karena itu, perlu ada perhatian serius dalam mengatasi masalah privasi di IoT untuk melindungi hak privasi pengguna.

Perlindungan privacy

Masalah privasi sebagian besar berasal dari operasi melalui internet, memaparkan informasi rahasia kepada penyerang. Dalam kasus IoT, tidak hanya pengguna yang terpapar pelanggaran privasi, tetapi semua orang yang ada di lingkungan juga terpapar risiko. Selain itu, karena menjamurnya aplikasi IoT di berbagai lokasi, pengguna memerlukan perlindungan atas informasi pribadi dan rahasia mereka yang terkait dengan lokasi, perilaku, dan komunikasi mereka dengan orang lain. Oleh karena itu, privasi pengguna harus dijaga (Sicari et al., (2015) Huang et al., (2012) membahas metode yang memungkinkan pengguna untuk mengontrol data pribadi mereka yang dikumpulkan dan diakses selain untuk mengetahui siapa yang mengumpulkan dan mengakses data tersebut dan kapan proses tersebut terjadi. Semua ini terjadi melalui protokol yang diusulkan yang disebut kontrol akses yang dilindungi privasi yang dikendalikan pengguna yang bergantung pada kebijakan privasi k-anonimitas yang sadar konteks. Yang et al., (2011) mengemukakakn dua kategori yang diambil dari teknik privasi tradisional: Akses Diskresioner, yang membahas risiko privasi minimum untuk menghindari pengungkapan atau penyalinan informasi rahasia, dan Akses Terbatas, yang berupaya meminimalkan akses keamanan untuk mencegah kejahatan dan serangan yang tidak sah.

Wang et al., (2011) menganalisis risiko privasi yang terjadi ketika nama domain statis dialokasikan ke perangkat IoT tertentu dan mengusulkan DNS yang ditingkatkan perlindungan privasi (Sistem Nama Domain) untuk perangkat cerdas untuk mengautentikasi identitas pengguna asli dan menolak yang tidak sah. akses ke perangkat. Ukil et al., (2014) mengusulkan skema manajemen privasi yang ditujukan untuk membatasi pengungkapan data pribadi dan analisis konten sensitif. Skema ini memungkinkan pengguna untuk mempertimbangkan risiko berbagi informasi sensitif dan upaya untuk membuat sistem yang kuat untuk deteksi sensitivitas yang mengukur kuantitas konten privasi informasi, selain itu strategi yang diusulkan bersifat umum, yang memungkinkan berbagai sensor deret waktu dapat diadaptasi aplikasi berbasis data. Du et al., (2018) memperkenalkan dan mensurvei tantangan dari tiga isu penting yang terkait dengan analisis data, perdagangan, dan agregasi untuk data penting keamanan dan sensitif privasi, dan memperkenalkan mekanisme pelestarian privasi di IoT untuk meningkatkan privasi dan memenuhi kebutuhan fungsional yang dibutuhkan. Namun, untuk melindungi privasi lokasi pengguna dengan meminimalkan biaya untuk mendapatkan layanan yang diinginkan adalah strategi baru yang terintegrasi dari skema cache dan k-anonymous yang diusulkan oleh Hu et al., (2018). Karena pentingnya melindungi privasi di IoT, banyak teknik sudah diterapkan untuk melindungi berbagai serangan privasi. Teknik-teknik ini terutama dapat diklasifikasikan ke dalam empat kategori; autentikasi dan otorisasi, edge computing dan arsitektur plug-in, anonimisasi data, lupa digital, dan ringkasan data yang ditujukan untuk melindungi setiap aspek privasi. Menurut Seliem et al., (2018) skema perlindungan privasi yang paling menonjol di setiap kategori masalah privasi dirangkum di bawah ini:

p-ISSN : 2808-8751 e-ISSN : 2798-2513

Otentikasi dan Otorisasi

Dalam domain teknologi IoT, privasi pengguna merupakan hal yang sangat penting dan perlu diperhatikan. Salah satu risiko privasi yang harus ditangani adalah berbasis Otentikasi dan Otorisasi untuk memastikan informasi pribadi pengguna tidak diakses oleh pihak yang tidak berwenang. Beberapa teknik peningkatan privasi yang menonjol dalam domain autentikasi dan otorisasi adalah Otentikasi Ringan, Sidik Jari Perangkat, Protokol Kunci PAuth, dan SmartOrBAC. Teknik otentikasi ringan memastikan otentikasi dalam lingkungan terbatas dengan memanfaatkan metode enkripsi berdasarkan operasi XOR. Sedangkan teknik sidik jari perangkat menggunakan metode memberikan sidik jari unik kepada setiap perangkat dan memastikan otentikasi perangkat dengan memverifikasi pesan yang dihasilkan milik objek tertentu dan pengirim pesan adalah sah. Selain itu, Protokol Kunci PAuth dan SmartOrBAC juga merupakan teknik autentikasi yang dirancang khusus untuk IoT dengan batasan sumber daya. Protokol Kunci PAuth memastikan verifikasi ujung ke ujung melalui dua fase, yaitu fase pendaftaran pengguna dan fase otentikasi dalam komunikasi, sedangkan SmartOrBAC adalah teknik autentikasi sadar konteks yang mampu mengakomodasi kebutuhan jaringan IoT. Teknik-teknik tersebut dapat memastikan perlindungan privasi terhadap penyalahgunaan data dan meningkatkan keamanan sistem IoT secara keseluruhan (Sharaf et al., 2016; Bouij et al., 2015).

Arsitektur Edge Computing dan Plug-In

Kelas teknik otentikasi dan privasi berbasis komputasi tepi dan arsitektur plug-in sedang populer saat ini. Dalam kategori ini, ada berbagai skema yang menonjol seperti Paradigma Komputasi Tepi, Sistem Sadar Privasi (pawS), dan Sentry@HOME. Paradigma Komputasi Tepi memproses dan menyimpan data di tepi jaringan untuk memastikan privasi pengguna. Sementara itu, pawS adalah sistem yang dirancang untuk memastikan data tetap rahasia dengan menggunakan alat pemrosesan dan pengumpulan data yang memberi tahu pengguna apa yang sedang diproses dan dikumpulkan. Sentry@HOME, di sisi lain, melindungi privasi di Smart Homes dengan menggunakan pendekatan yang berpusat pada pengguna dan menyebarkan data pribadi pengguna sesuai dengan kebijakan privasi yang ditentukan oleh mereka (Shi et al., 2016).

Anonimisasi Data

Anonimisasi data adalah sebuah teknik perlindungan privasi yang penting dalam era digital saat ini. Tujuan dari teknik ini adalah untuk menghapus informasi yang dapat diidentifikasi dari data, sehingga mencegah pengidentifikasian orang melalui data tersebut. Beberapa strategi yang dapat digunakan dalam anonimisasi data antara lain analisis risiko mendalam dan berbagi kunci berbasis identifikasi. Analisis risiko mendalam dapat dilakukan dengan menggunakan algoritma otentikasi yang dapat memverifikasi sumber file dengan menggunakan mekanisme kriptografi. Sedangkan, berbagi kunci berbasis identifikasi merupakan teknik yang menyediakan anonimisasi data melalui autentikasi timbal balik dan enkripsi komunikasi data dengan menggunakan informasi identifikasi pengguna atau perangkat sebagai kunci publik. Melalui teknologi ini, data bagian kecil dapat diungkapkan dengan penggunaan lapisan jaring pada peta untuk memanfaatkan data posisi (Shinzaki et al., 2016).

Pelupaan Digital dan Peringkasan Data

Kumpulan teknik terakhir yang menargetkan untuk memastikan privasi maksimum di IoT adalah teknik Melupakan Digital dan Peringkasan Data. Proses menghapus semua salinan kumpulan data yang digunakan selama komunikasi disebut melupakan data, sedangkan peringkasan data adalah penyediaan abstraksi kelas atas, yang menyembunyikan detail spesifik dari data dan mengurangi ukurannya. Dengan teknik seperti lupa digital dan peringkasan data, pengguna dapat menjadi lebih puas karena data dibuang, dan privasinya terjamin. Peringkasan Data terbagi menjadi dua kategori utama berdasarkan sifat transmisi dan perekaman data (Seliem et al., 2018). Kategori ini meliputi peringkasan waktu dan peringkasan spasial. Peringkasan waktu mengacu pada pengumpulan data sebagai fungsi waktu. Sebagai contoh, jika data dikumpulkan dengan kecepatan per detik, setelah peringkasan sementara, data akan dikumpulkan setelah kecepatan per jam. Sementara itu, peringkasan spasial mengacu pada pengumpulan data sebagai fungsi lokasi. Jika data direkam di semua lokasi berdasarkan GPS, setelah peringkasan spasial, data akan dikumpulkan hanya di kode pos tertentu.

Perlindungan Privasi di Lapisan IoT

p-ISSN : 2808-8751 e-ISSN : 2798-2513

Sama seperti skema perlindungan keamanan yang dianalisis dari perspektif setiap lapisan tergantung pada aplikasi dan strukturnya, teknik perlindungan privasi juga dapat diamati melalui perspektif lapisan dengan mempertimbangkan teknik yang berbeda di setiap lapisan. Karena lapisan fisik mengandung komponen perangkat keras, lapisan ini kurang rentan terhadap serangan privasi dan lebih rentan terhadap serangan keamanan karena tidak banyak teknik yang ditujukan untuk memecahkan masalah privasi di Lapisan Fisik. Teknik perlindungan privasi yang paling menonjol di setiap lapisan sebagaimana diadaptasi dari Seliem et al., (2018).

Perlindungan Privasi di Lapisan Aplikasi

Di lapisan aplikasi, masalah privasi hadir dalam dua bagian: di lapisan dukungan dan lapisan layanan. Lapisan dukungan bertanggung jawab atas komputasi tepi dan layanan analitik, sedangkan lapisan layanan bertanggung jawab untuk menyediakan dukungan yang diperlukan agar IoT berfungsi. Privasi data menjadi semakin penting dengan berkembangnya teknologi informasi. Oleh karena itu, ada berbagai teknik yang dapat dilakukan untuk memastikan privasi di Application Layer. Teknik tersebut antara lain Perlindungan Privasi Berbasis Preferensi, di mana entitas pihak ketiga digunakan untuk evaluasi preferensi privasi dan menyampaikannya ke penyedia layanan untuk memastikan tingkat privasi tertinggi berdasarkan preferensi yang ditetapkan. Selain itu, Kesadaran Privasi juga menjadi salah satu teknik yang efektif untuk meningkatkan privasi pengguna dengan membuat pengguna sadar akan potensi risiko privasi saat menggunakan perangkat mereka. Manajemen Keamanan juga menjadi teknik yang penting dalam menjaga privasi data, dengan penerapan tindakan perlindungan seperti mengelola kata sandi dan mengamankan informasi fisik. Beberapa peneliti seperti Ziegeldorf et al. dan Zyskind et al. juga telah mengusulkan mekanisme perlindungan privasi lainnya, seperti kesadaran dan kontrol pengguna, serta sistem manajemen data pengguna yang menggabungkan teknologi blockchain dengan solusi penyimpanan off-blockchain. Dengan berbagai teknik tersebut, diharapkan privasi pengguna dapat terjaga dengan baik di Application Layer. (Ziegeldorf et al., 2013; Zyskind et al., 2015)

Alcaide et al., (2013) mengusulkan protokol autentikasi anonim berbasis target terdistribusi untuk aplikasi IoT yang bergantung pada sistem kredensial multi-pertunjukan. Di sisi lain, Doukas et al., (2012) mengusulkan sebuah sistem berdasarkan solusi kunci publik yang melindungi data di perangkat IoT dengan menggunakan gateway IoT. Karya lain oleh Nguyen et al. (2015) membahas analisis teknik kriptografi kunci-bootstrap di IoT dan mengusulkan penggunaan protokol perjanjian kunci berbasis biometrik untuk menjaga privasi. Selain itu, format standar untuk mendeskripsikan data di IoT juga telah diusulkan, yang mencakup informasi pribadi dan menggunakan enkripsi, anonimitas, meminimalkan data, otentikasi untuk perlindungan privasi. Semua teknik ini memastikan keamanan data pada aplikasi layer dengan menggabungkan kriptosistem simetris maupun asimetris dan teknologi transmisi bersertifikat.

Perlindungan Privasi di Lapisan Jaringan

Lapisan jaringan berisi data yang dikirim sepanjang waktu dari satu host ke host lain yang terletak di jaringan yang berbeda, selain itu bertanggung jawab untuk perutean paket. Karena transmisi nirkabel dilakukan melalui internet, lapisan ini sangat rentan terhadap risiko pencurian data dan kompromi informasi pribadi. Karena alasan ini, beberapa fitur privasi yang diadopsi di lapisan ini juga memastikan privasi data di atas yang lainnya. Namun, dalam arah menyediakan keamanan dan privasi dalam komunikasi IoT, Gessner et al., (2012) menjelaskan sekelompok komponen keamanan yang meningkatkan kepercayaan untuk infrastruktur IoT. Dalam memastikan privasi di lapisan jaringan, ada beberapa teknik penting yang perlu diperhatikan. Pertama, otentikasi end-to-end digunakan untuk memastikan transmisi data yang aman dan rahasia dari satu ke yang lain. Autentikasi ujung ke ujung ini mencakup metode seperti perjanjian kunci, antarmuka Kunci Publik, dan perutean aman.

Bonetto et al. (2012) merekomendasikan penggunaan perangkat tepercaya untuk membongkar proses komputasi, sedangkan Weber et al. (2010) mengusulkan sebuah pendekatan untuk manajemen identitas dan akses yang berfokus pada komunikasi aman end-to-end dan masalah privasi pengguna. Selain itu, Henze et al. (2016) membahas strategi penegakan privasi berbasis pengguna untuk layanan berbasis cloud, dan González et al. (2016) menyarankan protokol agregasi pelestarian privasi (PAgIoT) untuk pengaturan IoT yang memungkinkan agregasi multi-atribut dalam satu set elemen dengan fokus pada korelasi nilai perlindungan privasi. Kedua, virtualisasi jaringan digunakan untuk meminimalkan risiko operasi yang tidak pantas dan tidak sah di lapisan jaringan. Ini dilakukan dengan mengurangi kompleksitas manajemen jaringan sehingga mengurangi kemungkinan pelanggaran privasi. Ketiga, protokol IPv6

p-ISSN : 2808-8751 e-ISSN : 2798-2513

diterapkan di lapisan jaringan untuk melindungi data dari kesalahan penanganan atau perusakan. IPv6 mempekerjakan mekanisme keamanan yang diwariskan dalam lapisan jaringan dan memungkinkan dukungan untuk pertahanan yang sukses (Shen et al., 2016). Selain itu, IPv6 memberikan privasi dengan secara otomatis menggunakan pengaturan acak untuk akhiran alamat IPv6 untuk menyembunyikan alamat MAC atau nomor pengenal apa pun saat terhubung ke Internet.

Perlindungan Privasi di Lapisan Persepsi

Karena lapisan persepsi berisi semua data rekaman sensor, penting untuk melindunginya dari pelanggaran privasi untuk menghindari penyalahgunaan data yang direkam oleh sensor. Teknik-teknik untuk memastikan privasi di lapisan jaringan mencakup berbagai risiko privasi seperti pengambilan simpul, informasi berbahaya, dan masalah otentikasi simpul. Beberapa teknik yang digunakan untuk mengatasi risiko ini adalah jamming RFID selektif, yang mencegah kebocoran privasi pada tag berbiaya rendah, dan Algoritma Kunci Nonlinier untuk Enkripsi Data, yang mengamankan pertukaran data dan menjamin transmisi data yang aman. Algoritma ini membutuhkan daya komputasi yang sangat rendah dan memberikan tidak hanya keamanan yang tinggi tetapi juga transmisi yang cepat. Selain itu, Mahmood et al. (2016) telah menyajikan metode untuk perangkat IoT untuk melindungi komunikasi end-to-end pengguna dari serangan DoS terdistribusi menggunakan enkripsi ringan. Li et al. (2017) juga mengusulkan protokol otentikasi ringan menggunakan metode enkripsi kunci publik untuk perlindungan aplikasi kota pintar. Semua teknik ini dapat membantu melindungi privasi pengguna di lapisan jaringan IoT.

Saluran aman menggunakan IPSec dapat memberikan perlindungan terhadap privasi dengan memastikan otentikasi dan enkripsi data. Dalam implementasinya, IPSec juga terbukti lebih efisien dalam memastikan privasi dibandingkan keamanan lapisan tautan IEEE 802.15.4 di IoT (Raza et al., (2012)). Selain itu, kriptografi juga digunakan dalam melindungi privasi di lapisan persepsi dengan menawarkan kerahasiaan, keaslian, dan integritas data. Protokol yang digunakan dalam kriptografi untuk lapisan persepsi mencakup tanda tangan digital dan nilai hash unik. Raza et al., (2012) menerapkan pertukaran kunci Diffie Hellman dan hashing di smart home untuk melindungi privasi dalam konten terdesentralisasi. Semua ini menunjukkan betapa pentingnya kriptografi dalam memastikan privasi pada berbagai lapisan dalam lingkungan IoT. Banyak peneliti terlibat dalam mengeksplorasi berbagai strategi dan metode untuk memastikan privasi, Sen et al., (2018) membedakan antara definisi privasi dan keamanan dalam pekerjaan mereka, selain itu, menunjukkan beberapa berbagai teknik yang digunakan untuk mencapai privasi. persyaratan dengan menyebutkan beberapa keuntungan dan kerugian dari metode yang ditujukan.

Prinsip Privasi Berdasarkan Desain

Dalam visi masa depan di mana semuanya terhubung, data dapat dikumpulkan dari mana saja tanpa sepengetahuan pengguna. Untuk memastikan keamanan dan privasi di lingkungan Internet of Things (IoT), prinsip Privacy-by-Design harus diterapkan oleh peneliti dan pengembang. Konsep ini mendorong strategi rekayasa keamanan yang mempertimbangkan persyaratan privasi sebagai tujuan organisasi dalam proses bisnis dan identifikasi. Fabiano (2013) menyajikan tujuh prinsip utama yang harus diikuti, seperti mengambil tindakan proaktif untuk mencegah masalah privasi selama fase desain, melindungi privasi secara otomatis dalam proses bisnis, menyematkan privasi ke dalam desain, memastikan fungsionalitas penuh di akhir komunikasi, menjamin keamanan end-to-end, memastikan transparansi bagi pengguna, dan menghormati privasi pengguna. Dengan mengikuti prinsip-prinsip ini, IoT dapat menghadirkan lingkungan yang aman dan dapat dipercaya bagi pengguna. Privacy-by-Design melindungi privasi di IoT dengan berfokus pada sensor IoT, peraturan hukum, komputasi awan, dan analisis data masif (Porambage et al., (2016).

Dalam bidang IoT, banyak peneliti telah mencoba untuk mencari solusi untuk mengelola perangkat IoT melalui halaman web atau aplikasi. Piyare et al. (2011) mempertimbangkan solusi berbasis server web yang murah, fleksibel, dan dapat diandalkan untuk mengontrol perangkat rumah. Namun, sistem Piyare hanya dapat mengalihkan dan mengontrol peralatan dan perangkat rumah tangga, dan hanya bekerja pada smartphone Android atau tablet Android, tanpa mempertimbangkan privasi pengguna. Dhake et al. (2016) mengusulkan penggunaan ASP.NET untuk menciptakan server web yang dapat mengontrol smart home melalui aplikasi Android, namun sistem ini juga hanya berfungsi di smartphone Android. Shrestha et al. (2017) mengembangkan sistem smart home yang dapat dikontrol melalui aplikasi Android dan halaman web, dengan fokus pada autentikasi pengguna untuk melindungi keamanan. Namun, solusi-solusi ini hanya

p-ISSN : 2808-8751 e-ISSN : 2798-2513

difokuskan pada pengendalian dan pemantauan perangkat, dan mungkin tidak dapat mengontrol perangkat IoT lain yang berbeda dan tidak mempertimbangkan privasi pengguna. Oleh karena itu, solusi-solusi tersebut memiliki beberapa keterbatasan dan perlu ditingkatkan dalam hal privasi pengguna dan fungsionalitas yang lebih luas. Ada berbagai platform (aplikasi) yang dirancang untuk menyediakan pengelolaan perangkat IoT, seperti RestThing (Yan et al., 2014) dan EcoDiF (Pires et al., 2014), yang bertujuan untuk memantau dan mengontrol perangkat IoT melalui layanan web. Namun, solusi-solusi tersebut masih memiliki keterbatasan dalam menjaga privasi pengguna. Oleh karena itu, masih diperlukan pengembangan sistem yang memungkinkan pengguna IoT mengontrol perangkat mereka dengan menjaga privasi dan melindungi informasi pribadi mereka.

MODEL YANG DIUSULKAN

Gagasan untuk membuat "User-Interface Berbasis Web untuk Perangkat Internet of Things" yang ramah pengguna muncul, yang akan memungkinkan pengguna IoT untuk mengontrol dan mengelola perangkat IoT mereka. Dalam istilah paling sederhana, ini adalah cara pengguna dan perangkat IoT-nya berinteraksi untuk menjaga privasi.

Platform yang Diusulkan

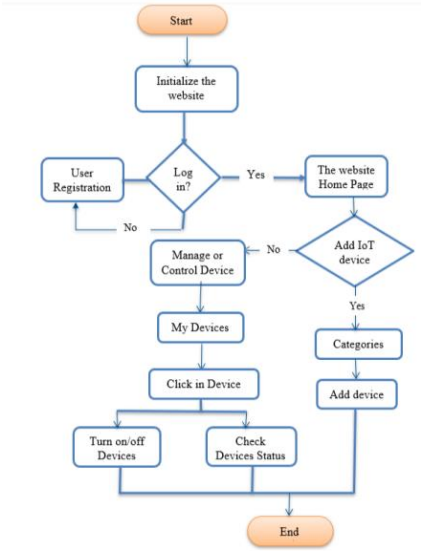
Penelitian ini mengusulkan sistem web-based untuk mengatasi masalah privasi dan User-Interface pada perangkat IoT. Tujuannya adalah untuk meningkatkan persepsi pengguna terhadap perangkat IoT dan privasi mereka. Sistem ini dapat diakses melalui URL dan berfungsi untuk mengontrol perangkat IoT dari jarak jauh, mengakses status perangkat, mengontrol informasi yang dikumpulkan, dan mengatur preferensi privasi untuk perangkat IoT tertentu. Sistem ini dapat diakses melalui sistem operasi apa pun dan tidak memerlukan unduhan aplikasi. Aplikasi web yang diusulkan memiliki beberapa fitur signifikan. Pertama, pengguna dapat mengakses informasi tentang perangkat yang terhubung dengan IoT melalui situs web, termasuk status perangkat. Untuk dapat mengakses informasi perangkat, pengguna harus menghubungkan perangkat ke aplikasi web terlebih dahulu. Selanjutnya, pengguna dapat mengontrol berbagai perangkat yang terhubung dengan IoT dari jarak jauh melalui situs web, seperti menghidupkan/mematikan perangkat atau menjadwalkan tugas untuk perangkat tertentu pada waktu tertentu di berbagai lokasi, seperti rumah, tempat kerja, dan kendaraan. Selain itu, pengguna dapat mengontrol dan mengelola informasi yang dikumpulkan oleh perangkat IoT tentang diri mereka melalui situs web. Ini memungkinkan pengguna untuk memantau data mereka dan mengatur preferensi privasi untuk setiap perangkat berdasarkan lokasi perangkat. Fitur lainnya dari aplikasi web ini termasuk kemampuan untuk melihat operasi perangkat yang terhubung secara real time, seperti pending dan eksekusi, serta mengelola perangkat lunak dan izin perangkat, seperti mengganti kata sandi. Karena beberapa sistem yang diusulkan sebelumnya mungkin memiliki beberapa keterbatasan, sehingga tidak memungkinkan untuk mengontrol atau mengelola perangkat IoT lain yang berada di domain lain yang berbeda. Selain itu, beberapa solusi memerlukan beberapa tingkat keterampilan teknis dari pengguna, dan beberapa di antaranya bekerja dengan sistem operasi tertentu atau pada perangkat tertentu. Selain itu, beberapa manajemen perangkat IoT sebelumnya diusulkan hanya untuk tujuan pengendalian dan pemantauan dan tidak berfokus pada perlindungan privasi pengguna IoT. Sedangkan situs web yang diusulkan dimaksudkan untuk fokus pada penyelesaian kelemahan ini pada pekerjaan sebelumnya dengan lebih fokus pada perlindungan privasi pengguna IoT.

Detil Deskripsi

Lingkungan situs web "User-Interface Berbasis Web untuk Manajemen Perangkat IoT" terdiri dari perangkat IoT, situs web WordPress, modul permintaan dan eksekusi fungsi, serta basis data. Situs web menggunakan bahasa Node/JavaScript dan pengguna IoT berkomunikasi dengan perangkat melalui API standar melalui situs web. Setiap perangkat IoT harus terhubung ke aplikasi web dengan API terpisah untuk memanggil pemicu khusus dengan perangkat, dan situs web menyediakan User-Interface untuk mengelola dan mengontrol perangkat IoT. Dengan standarisasi interaksi antara situs web dan perangkat IoT, perangkat IoT dapat dikelola dari satu platform tanpa memerlukan aplikasi terpisah. Modul permintaan dan eksekusi fungsi memungkinkan komunikasi antara aplikasi web dan perangkat IoT melalui Internet. Ketika pengguna meminta akses ke situs web, modul permintaan fungsi menghubungkan dengan perangkat IoT terkait dan menerima respons yang menampilkan fungsionalitas perangkat. Informasi tentang perangkat IoT dan fungsionalitasnya disimpan dalam database MySQL untuk memudahkan akses di masa depan. Setelah modul permintaan fungsi menerima respons, modul eksekusi fungsi mengirimkan permintaan eksekusi ke perangkat IoT. Permintaan eksekusi mengidentifikasi fungsi yang harus dijalankan oleh perangkat IoT dan

p-ISSN : 2808-8751 e-ISSN : 2798-2513

ditampilkan di User Interface pada situs web. Pengguna dapat mengakses situs web dan mengelola perangkat IoT mereka dari mana saja dengan menggunakan kredensial rahasia untuk masuk ke akun mereka.



Gambar 1 – Kerangka Usulan Data Situs Web

Database MySQL digunakan untuk menyimpan informasi tentang perangkat IoT, fungsionalitas, data historis, dan analitik, serta struktur pendukung yang dibutuhkan. Pengguna dapat memantau data yang diambil dari perangkat IoT tertentu dan mengatur preferensi privasi mereka untuk setiap perangkat yang terhubung berdasarkan lokasi perangkat. Situs web menyediakan layanan analitik untuk memanfaatkan data yang dikumpulkan dan menampilkan data historis tentang permintaan dan eksekusi fungsi untuk setiap perangkat IoT. Pengguna dapat menggunakan perangkat seluler atau komputer untuk menghubungkan perangkat IoT mereka ke situs web melalui Internet atau jaringan publik lainnya untuk mengelola dan mengontrolnya. Untuk menghubungkan perangkat IoT ke aplikasi web, pengguna memasukkan detail perangkat IoT di aplikasi web dan memilih kategori yang tepat untuk perangkat tersebut. Kemudian, mereka dapat mengakses informasi tentang perangkat yang terhubung. Modul permintaan dan eksekusi fungsi yang terhubung ke perangkat IoT melalui Internet dan disimpan dalam database MySQL memungkinkan pengguna untuk mengelola perangkat IoT mereka dari mana saja melalui aplikasi web.

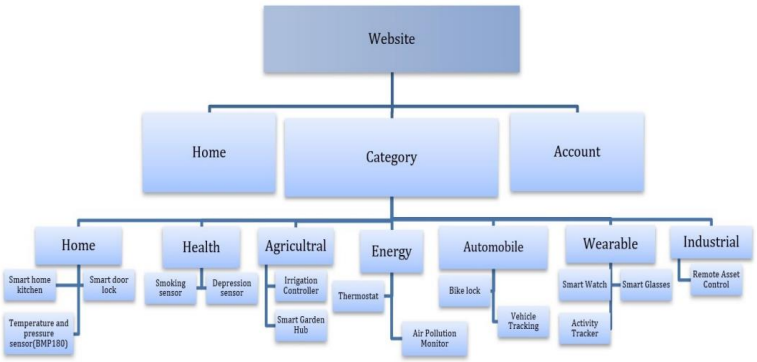
Prototipe yang Diusulkan

Pada tahap ini, deskripsi yang disebutkan di atas tidak semuanya diterapkan karena perlu mengintegrasikan API untuk perangkat IoT untuk menghubungkannya langsung ke aplikasi web. Padahal, setiap perangkat memiliki seperangkat kemampuan, protokol, perintah, dan fungsi yang berbeda, yang digunakan untuk mengkomunikasikan pesan antara perangkat dan platform. Oleh karena itu, ada kebutuhan untuk mengintegrasikan API terkait untuk setiap perangkat, yang mempersulit implementasi semua prosedur pada tahap ini. Namun, prototipe telah dibuat yang dapat digunakan untuk mendemonstrasikan dan mengevaluasi konsep "Aplikasi Web" yang dapat mengelola perangkat IoT untuk menjaga privasi.

Struktur Situs Web Prototipe

Website dibuat dengan menggunakan program Wordpress (open source) sebagai Content Management System (CMS) yang mencakup arsitektur plugin dan fitur sistem template. Itu dapat diakses dengan memasukkan alamat URL-nya (http://iotprivacycontrol.com/). Alasan di balik penggunaan program WordPress adalah kompatibilitas dengan berbagai mesin pencari, dan kemampuan untuk menyediakan berbagai kemampuan untuk kebutuhan, seperti memutakhirkan situs dengan mudah dan mendapatkan keuntungan dari desain web yang responsif.

p-ISSN : 2808-8751 e-ISSN : 2798-2513



Gambar 2 - Struktur Aplikasi Web

Aplikasi web berisi sistem login untuk tujuan otentikasi pengguna yang memungkinkan pengguna untuk login dengan kredensial rahasia untuk hanya mengizinkan pengguna yang diautentikasi untuk menggunakan situs web dan melindungi sumber dayanya dari pengguna yang tidak sah. Aplikasi web saat ini berisi tiga halaman utama, yaitu halaman Beranda tempat pengguna dapat menavigasi ke halaman lain, halaman Kategori tempat pengguna dapat memilih kategori spesifik perangkat IoT mereka, dan halaman Akun tempat pengguna dapat mengakses/masuk ke akun mereka. Situs web adalah pemantauan waktu nyata, aplikasi web responsif yang berfungsi di setiap perangkat yang dapat mengakses internet (mis., ponsel, tablet, dan desktop), dan menerapkan pengalaman pengguna waktu nyata.

Instrumen dan Metode

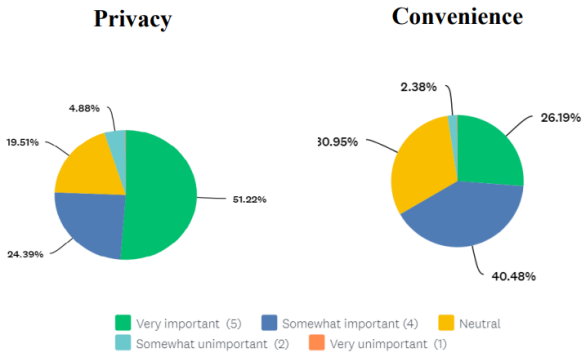
Penelitian ini dilakukan dengan menggunakan dua metode: studi eksperimental dan survei online. Dalam studi eksperimental, peserta diminta untuk menggunakan situs web User-Interface Berbasis Web untuk Perangkat IoT yang telah diuji secara kuantitatif untuk mengevaluasi kinerja peserta dalam kelompok eksperimen. Situs web ini dapat diakses melalui tautan (http://iotprivacycontrol.com/) dan dapat berinteraksi dengan perangkat IoT di lokasi mana pun. Selain itu, survei dilakukan secara online menggunakan Survey Monkey untuk menilai persepsi peserta tentang privasi mereka saat menggunakan perangkat IoT. Peserta diinstruksikan untuk membaca dan menyetujui formulir Informed Consent sebelum melakukan tugas-tugas yang ditentukan, seperti menambahkan kunci pintu pintar ke akun mereka dan mendapatkan informasi tentang data yang dikirim oleh sensor BMP180 yang terhubung dengan IoT.

DATA ANALYSIS AND IMPLICATION

Analisis Primer

Statistik deskriptif

Menggunakan skala Likert 5 poin (1 = “Sangat Tidak Penting”, 5 = “Sangat Penting”), para peserta mengungkapkan pandangan mereka tentang pentingnya privasi dan kenyamanan saat menggunakan perangkat pintar. Hasilnya ±50% dari peserta percaya bahwa privasi sangat penting saat menggunakan perangkat pintar, dan kurang dari 1/3 peserta percaya bahwa kenyamanan sangat penting saat menggunakan perangkat pintar.



p-ISSN : 2808-8751 e-ISSN : 2798-2513

Gambar 3 – Pentingnya Privasi dan Kenyamanan

Tabel 1. Kategori Peserta Berdasarkan Penggunaan Perangkat IoT

PARTICIPANTS' GRPOUPS	Low-Frequency Users		Moderate Users		Intensive Users		
At	0 – 1 Hour	4 – 6 Hours	7 – 10 Hours	11 -14 Hours	15 – 20 Hours	More Than 20 Hours	Total
Home	**2.33%**	**41.86%**	**23.26 %**	**11.63%**	**13.95%**	**6.98%**	**100%**
	1	**18**	**10**	**5**	**6**	**3**	**43**

Dari hasil survei, sekitar 50% peserta menganggap penting untuk dapat mengontrol informasi yang dikumpulkan oleh perangkat IoT tentang diri mereka, sedangkan lebih dari sepertiga peserta menemukannya cukup penting. Selain itu, lebih dari sepertiga peserta percaya bahwa pemberitahuan saat informasi pribadi mereka dikumpulkan dapat membantu melindungi data pribadi mereka, dan lebih dari 40% peserta juga menganggap tindakan ini penting. Lebih dari 45% peserta percaya bahwa meminta izin mereka sebelum mengumpulkan informasi dengan perangkat IoT adalah sangat penting, sementara 19% menganggapnya penting. Perlu dicatat bahwa peserta dalam survei ini dibagi menjadi tiga kelompok berdasarkan jumlah penggunaan perangkat IoT mereka.

Statistik Inferensial

Semua analisis statistik dihitung dengan menggunakan perangkat lunak statistik IBM SPSS Statistics dan mengasumsikan tingkat signifikansi $p<0,05$. Untuk menguji hipotesis H1 berhipotesis bahwa ketika pengguna menggunakan perangkat pintar, privasi lebih penting bagi mereka daripada kenyamanan. Uji-t dependen dilakukan pada sampel berpasangan untuk membandingkan cara privasi dan kenyamanan untuk menentukan apakah ada perbedaan yang signifikan secara statistik di antara keduanya. Ditemukan bahwa privasi ($M = 4.23$, $SD = .922$) dan kenyamanan ($M = 3.86$, $SD = .861$) berbeda secara signifikan ($p = 0.010 < 0.05$), dan nilai rata-rata privasi lebih tinggi daripada nilai rata-rata dari kenyamanan. Mengacu pada H2, bahwa tidak ada pengaruh jumlah penggunaan perangkat IoT oleh pengguna terhadap pentingnya tindakan berikut bagi mereka untuk melindungi informasi pribadi mereka yang ditangkap oleh perangkat IoT: mampu mengontrol informasi apa yang dikumpulkan tentang mereka oleh perangkat IoT, diberi tahu saat informasi pribadi mereka dikumpulkan oleh perangkat IoT, dan meminta izin mereka untuk mengumpulkan informasi mereka oleh perangkat IoT sebelum dikumpulkan. Kelompok peserta yang teridentifikasi (pengguna frekuensi rendah, pengguna sedang, dan pengguna intensif) dimanfaatkan dalam melakukan uji non-parametrik (uji Kruskal-Wallis) untuk menentukan apakah ada perbedaan yang signifikan secara statistik antara jumlah penggunaan IoT (rendah- pengguna frekuensi, pengguna sedang, dan pengguna intensif) tentang pentingnya tindakan tersebut. Hasil yang tidak signifikan ditemukan pada nilai p ($p > 0,05$). Oleh karena itu, tidak ada perbedaan yang signifikan secara statistik antara tingkat penggunaan IoT untuk semua tindakan, dan semua tindakan penting bagi sebagian besar peserta berdasarkan nilai rata-rata. Untuk menilai kepuasan peserta terhadap prototipe (situs web), tiga faktor dihasilkan; Organisasi web ($M = 4.12$, $SD = .731$), Kemudahan navigasi situs web ($M = 4.30$, $SD = .741$), dan User-Interface ($M = 4.35$, $SD = .650$) pada skala Likert 5 poin (dari "1 = sangat tidak puas" hingga "5 = sangat puas"). Sehubungan dengan H3, hipotesisnya adalah peserta akan puas dengan organisasi situs web, kemudahan navigasi situs web, dan User-Interface saat mereka mengalaminya didukung berdasarkan tanggapan peserta dan nilai rata-rata dari faktor-faktor ini.

Pemahaman Peserta terhadap Website (User-Interface Web App)

Hasil survei menunjukkan bahwa survei terdiri dari tiga tugas yang masing-masing memiliki tiga pertanyaan terbuka dengan opsi jawaban benar atau salah. Untuk memudahkan analisis, tag nomor satu diberikan untuk jawaban benar dan nol untuk jawaban salah. Meskipun tiga peserta tidak menyelesaikan tugas, masih dapat mengumpulkan data dari 38 peserta. Pada tugas pertama, 35 dari 38 peserta dapat menjawab dengan benar mengenai jumlah perangkat yang terhubung ke akun website. Pada tugas kedua, 36 dari 38 peserta dapat mengikuti instruksi dan menjawab dengan benar mengenai jumlah pembacaan sensor

p-ISSN : 2808-8751 e-ISSN : 2798-2513

suhu dan tekanan yang tersedia. Pada tugas ketiga, hanya satu peserta yang menjawab dengan salah mengenai pembacaan suhu untuk tanggal dan waktu tertentu. Selain itu, kepuasan peserta terhadap prototipe situs web juga dievaluasi menggunakan skala Likert 5 poin, dengan skor rata-rata peserta sebesar 4,07 untuk organisasi situs web, 4,23 untuk kemudahan navigasi situs web, dan 4,30 untuk antarmuka yang ramah pengguna.

Penggunaan Perangkat IoT

Tabel 2 menunjukkan bahwa banyak peserta dari 43 peserta menggunakan perangkat IoT untuk tujuan yang berbeda, seperti produk Smart Home yang biasanya membantu menghemat waktu, biaya, dan tenaga. Studi ini menunjukkan bahwa sekitar 40% peserta menggunakan perangkat IoT mereka untuk tujuan Smart Home, dan sekitar 27% peserta menggunakan produk pelacakan Kendaraan yang dapat digunakan untuk tujuan keamanan jika kendaraan mereka dicuri. Sedangkan persentase yang paling signifikan adalah sekitar 70% peserta menggunakan perangkat IoT untuk keperluan hiburan, yang meliputi beberapa perangkat IoT seperti Smart TV, game virtual, Smart toys, dan Smart Wristband. Gaya hidup juga merupakan salah satu tujuan paling umum orang menggunakan perangkat IoT untuk meningkatkan kehidupan mereka. Studi ini menunjukkan bahwa lebih dari 60% peserta cenderung menggunakan perangkat IoT mereka untuk gaya hidup. Selain itu, untuk pemantauan kesehatan, orang dapat menggunakan perangkat pelacak pintar untuk melacak pola tidur dan jadwal pemeriksaan. Jadi, seperti yang terlihat dalam penelitianini, sekitar 42% peserta menggunakan perangkat IoT untuk memantau kesehatan. Namun, kurang dari 5% peserta tidak memiliki perangkat IoT sama sekali. Studi ini menunjukkan bahwa 60% dari peserta tidak menggunakan salah satu aplikasi manajer IoT tipikal dan rasio rendah yang serupa dengan aplikasi manajemen IoT lainnya, hasilnya tersedia di Tabel 2. Untuk mengetahui bagaimana peserta memahami perangkat IoT, jenis informasi yang akan ditangkap oleh perangkat IoT tertentu seperti Smart Tv, dan smartphone, ditanyakan.

Tabel 2 Penggunaan Perangkat IoT

IoT Devices' usage	Number	Percent
Purposes		
Smart Home	18	41.86%
Vehicle Tracking	12	27.91%
Entertainment	30	69.77%
Lifestyle	26	60.47%
Health monitoring	18	41.86%
None (do not have an IoT device)	2	4.65%
IoT management Application		
Wink		
SimpliSafe Home Security	4	9.30%
Yonomi	4	9.30%
ADT Control	0	0.00%
Olisto	4	9.30%
None	1	2.33%
Do not have an IoT device	26	60.47%
	4	9.30%

Sikap Privasi Peserta

Kepedulian peserta tentang privasi dalam kehidupan sehari-hari juga ditanyakan untuk mengevaluasi persepsi privasi peserta secara umum. Menggunakan skala Likert 4 poin (1 = "Tidak sama sekali", 4 = "Sangat Peduli"), peserta mengungkapkan pandangan mereka. Dengan demikian, dari nilai rata-rata dan standar deviasi (M > 2,5) diindikasikan bahwa sebagian besar peserta agak khawatir dengan privasi mereka secara umum. Persepsi peserta tentang peringkat otoritas yang bertanggung jawab, dari pemerintah, produsen perangkat IoT, atau pengguna IoT juga di eksplorasi dalam perlindungan privasi pengguna saat menggunakan perangkat IoT. Kesediaan peserta untuk mengambil tindakan dalam rangka melindungi informasi pribadinya yang ditangkap oleh perangkat IoT menggunakan skala Likert 5 poin, peserta mengungkapkan pandangan mereka tentang berbagai aspek terkait pengelolaan IoT perangkat dan mengurangi risiko pelanggaran privasi, ketika mereka berasumsi bahwa mereka tinggal di smart home yang berisi berbagai perangkat dan sensor IoT yaitu: Smart Tv, Smart light, Smart Thermostat, dan Smartwatch) yang menangkap berbagai jenis informasi mereka. Selain itu, mayoritas peserta (sekitar 74%) lebih memilih

p-ISSN : 2808-8751 e-ISSN : 2798-2513

menggunakan situs web untuk mengelola perangkat IoT mereka daripada aplikasi tertentu. Sejumlah besar peserta (sekitar 70%) lebih suka menggunakan satu platform untuk mengelola semua perangkat IoT mereka dan mengurangi risiko pelanggaran privasi saat mereka tinggal di smart home yang berisi berbagai perangkat IoT, dan sensor.

Diskusi

Beberapa penelitian sebelumnya telah menyelidiki faktor-faktor yang memengaruhi pendapat orang tentang adopsi IoT. Privasi menjadi alasan utama mengapa pengguna enggan menggunakan teknologi ini. Sebuah survei menunjukkan bahwa 75% orang tidak percaya dengan cara berbagi data pada perangkat terhubung. Temuan dari uji hipotesis menunjukkan bahwa privasi lebih penting daripada kenyamanan bagi peserta saat menggunakan perangkat pintar. Meskipun ada kekhawatiran mengenai privasi, orang masih membeli perangkat IoT dan jumlah penjualan meningkat, para peneliti tertarik untuk mengidentifikasi apakah tingkat penggunaan perangkat IoT memengaruhi sikap pengguna dalam tindakan untuk melindungi privasi mereka. Uji hipotesis menunjukkan tidak ada hubungan antara tingkat penggunaan dan tindakan melindungi privasi. Hal ini menunjukkan bahwa pengguna perangkat IoT, terlepas dari tingkat penggunaannya, masih membutuhkan alat yang membantu mereka melindungi informasi pribadi dan privasi. Para ahli kemudian memperkenalkan prototipe situs web yang dapat membantu pengguna melindungi privasi mereka. Uji hipotesis menunjukkan sebagian besar peserta puas dengan prototipe tersebut, dan situs web ini dapat dioptimalkan di masa mendatang untuk membantu pengguna melindungi privasi mereka saat menggunakan perangkat IoT.

Di sisi lain, para ahli telah menjelaskan mengapa orang masih membeli perangkat ini meskipun mereka tidak mempercayainya; orang mungkin tidak memahami sejauh mana data yang dikumpulkan oleh perangkat pintar, orang mungkin menganggap pertukaran itu sepadan, tidak ada lagi pilihan bagi konsumen, orang mengira pemerintah akan mengurusnya, dan beberapa orang tidak cukup peduli tentang privasi untuk mengambil tindakan tentang hal itu. Selain itu, sebelas wawancara semi-terstruktur dilakukan dengan pemilik Smart Home untuk mengetahui alasan mereka di balik pembelian perangkat IoT, keyakinan akan risiko privasi smart home, dan bagaimana mereka melindungi privasi mereka dari entitas eksternal. Tema berulang dari penelitian ini menunjukkan bahwa pengguna menghargai kenyamanan dan keterhubungan yang dapat memengaruhi opini privasi mereka, manfaat yang dirasakan dari entitas eksternal memengaruhi opini pengguna tentang siapa yang harus mengakses smart home mereka, dan pengguna memercayai produsen perangkat IoT dalam melindungi mereka. privasi tanpa kesadaran akan potensi pembelajaran mesin untuk mengungkap informasi sensitif dari data non-audio/visual.

Meskipun IoT dapat meningkatkan kenyamanan hidup pengguna, dan kebanyakan orang mungkin lebih memilih kenyamanan daripada potensi risiko, hal itu juga melanggar privasi. Pilihan tipe data peserta yang akan ditangkap oleh perangkat IoT tertentu dipilih, seperti Smart Thermostat, Smart TV, dan smartphone tidak akurat. Sehingga dapat disimpulkan bahwa sebagian besar peserta tidak memahami perangkat IoT dan jenis data apa yang dapat dirasakan tentangnya oleh perangkat tertentu, yang menegaskan bahwa kurangnya kesadaran pengguna IoT tentang perangkat IoT dan kebutuhan mereka untuk menjadi lebih berpengetahuan dan menyadari tentang perangkat IoT untuk melindungi privasi mereka. Temuan ini memberikan bukti ketidaktahuan beberapa pengguna tentang risiko privasi terkait penggunaan perangkat yang terhubung ke Internet, termasuk perangkat IoT, dan menyarankan kebutuhan untuk memberikan konsep baru yang dapat melindungi privasi pengguna tanpa mengubah pendapat mereka tentang tujuan kenyamanan penggunaan IoT. perangkat.

Dalam satu sisi, ahli telah menjelaskan mengapa orang masih membeli perangkat IoT meskipun mereka tidak percaya pada keamanannya. Beberapa alasan yang mungkin termasuk ketidaktahuan pengguna tentang data yang dikumpulkan oleh perangkat, pandangan bahwa pertukaran privasi sepadan dengan kenyamanan dan keterhubungan yang ditawarkan, kurangnya alternatif lain bagi konsumen, keyakinan bahwa pemerintah akan mengatur masalah privasi, dan kurangnya kepedulian tentang privasi dari beberapa pengguna. Dalam penelitian lain, wawancara dengan pemilik Smart Home menunjukkan bahwa mereka memilih perangkat IoT untuk kenyamanan dan keterhubungan yang ditawarkan, dan percaya bahwa produsen perangkat akan melindungi privasi mereka. Namun, kurangnya kesadaran pengguna tentang jenis data yang dapat dikumpulkan oleh perangkat IoT tertentu menunjukkan kurangnya kesadaran tentang risiko privasi terkait penggunaan perangkat terhubung ke Internet. Oleh karena itu, diperlukan

p-ISSN : 2808-8751 e-ISSN : 2798-2513

konsep baru yang dapat melindungi privasi pengguna tanpa mengubah pandangan mereka tentang tujuan kenyamanan penggunaan perangkat IoT.

Dalam penelitian ini, ditemukan bahwa orang mungkin lebih memperhatikan privasi mereka saat menggunakan perangkat pintar dan beberapa dari mereka bahkan menghindari penggunaan perangkat pintar karena masalah privasi terkait perangkat yang terhubung ke Internet. Namun, orang yang lebih menghargai kenyamanan daripada privasi dalam menggunakan perangkat pintar disebabkan oleh banyak faktor berbeda yang dapat memengaruhi pendapat mereka termasuk kurangnya kesadaran mereka terhadap perangkat pintar. Berdasarkan analisis tambahan dari survei, ditemukan bahwa prototipe yang diusulkan adalah platform yang mudah diakses, dan dapat digunakan dengan mudah oleh para peserta dengan tingkat yang berbeda pendidikan dan tingkat yang berbeda dalam menggunakan perangkat IoT tanpa banyak pengalaman teknis. Selain itu, ditemukan juga penggunaan perangkat IoT yang semakin meluas, dan sebagian besar peserta sudah familiar dengan perangkat IoT.

Dengan menyediakan User-Interface berbasis web kepada pengguna IoT dapat memungkinkan mereka untuk mengumpulkan dan menghubungkan semua perangkat IoT mereka ke satu platform dan mengontrolnya dengan mudah dari mana saja seperti rumah, tempat kerja, dan kendaraan melalui platform tersebut. Fitur ini akan memungkinkan pengguna IoT untuk dapat menghubungkan semua perangkat IoT yang mereka gunakan untuk berbagai keperluan ke situs web dengan mudah. Selain itu, ditemukan bahwa para peserta percaya bahwa pengguna IoT bertanggung jawab untuk melindungi privasi mereka. Sehingga diperlukan fasilitas cara melindungi privasi mereka saat menggunakan perangkat IoT dengan menyediakan User-Interface aplikasi web yang sedang dikembangkan. Singkat kata, solusi yang diusulkan sangat penting untuk melindungi privasi pengguna dalam penggunaan perangkat IoT, karena mayoritas peserta mengkhawatirkan privasi mereka tentang data yang dideteksi saat menggunakan perangkat IoT. Solusi berupa situs web yang memungkinkan pengguna mengelola perangkat mereka di satu platform dapat membantu pengguna untuk melindungi privasi mereka, meskipun beberapa pengguna memilih untuk menggunakan perangkat fisik untuk mengelola beberapa perangkat IoT mereka. Speaker smart home seperti Amazon Echo dan Google Home juga digunakan untuk mengelola perangkat dan layanan dengan berbagai desain dan spesifikasi berdasarkan lokasi dan tujuan penggunaan.

3. HASIL DAN PEMBAHASAN

Limitasi

Dalam penelitian ini, ditemukan beberapa hal yang perlu diperhatikan. Pertama studi ini bisa mengalami bias karena mayoritas peserta, yaitu 60%, berusia antara 25 dan 34 tahun dan 86% dari mereka memiliki setidaknya gelar sarjana. Hal ini memberikan beberapa kesulitan untuk menggeneralisasi hasil karena populasi umum mungkin memiliki usia dan tingkat pendidikan yang berbeda. Kedua, lebih dari separuh peserta tidak menggunakan aplikasi apa pun untuk pengelolaan perangkat IoT, dan hal ini dapat memengaruhi pendapat mereka karena ini adalah pertama kalinya mereka mengalami platform semacam itu, sehingga mereka tidak memiliki latar belakang platform lain yang searah. Karenanya, informasi ini harus dipertimbangkan saat meninjau jawaban mereka terkait perbandingan dengan platform lain. Ketiga, para peserta diminta untuk membayangkan diri mereka sendiri ke dalam situasi hipotetis yang terbatas pada apa yang dapat mereka liput, dan ditemukan bahwa privasi lebih penting daripada kenyamanan saat menggunakan perangkat pintar, dan sebagian besar peserta sangat sensitif terhadap privasi. Oleh karena itu, penelitian ini bisa jadi cukup rentan terhadap bias ini karena skenarionya abstrak, dan peserta diminta untuk membayangkan diri mereka sendiri dalam situasi yang mungkin tidak mereka temui. Keempat, jumlah peserta hanya sedikit sehingga tidak memiliki data yang cukup untuk menggeneralisasi temuan ke seluruh populasi yang diinginkan. Terakhir, merancang dan mengimplementasikan situs web yang diusulkan akan menjadi tugas yang menantang karena beberapa alasan yang disebutkan di atas dalam bab situs web. Oleh karena itu, penelitian ini hanya mengembangkan prototipe eksperimental untuk memvalidasi kerangka kerja yang diusulkan. Prototipe disediakan dalam penelitian ini mencakup ide utama pengelolaan situs web IoT, dan tidak mencakup beberapa masalah potensial yang mungkin dihadapi pengguna IoT saat menggunakan situs web, seperti tantangan keamanan.

Google Home Hub dapat diaktifkan dengan suara dan melakukan tugas apa pun dari Asisten Google, ini memungkinkan pengguna untuk mengalirkan media dan musik dari ponsel. Akan t6etapi, perangkat ini tidak memiliki browser web, sehingga pengguna tidak dapat menarik gambar pencarian Google tertentu. Sebagian besar fungsi yang dapat dicapai oleh Google Home Hub adalah mengontrol

p-ISSN : 2808-8751 e-ISSN : 2798-2513

cahaya, mentransmisikan media, siaran, dan pesan, mengubah termostat, melihat kamera pintar, dan mengubah perangkat yang mendukung TV. Meskipun demikian, perangkat IoT seperti Google Home dapat mengumpulkan informasi pribadi tentang pengguna dan informasi ini dapat disimpan, digunakan, atau dijual tanpa izin pengguna. Oleh karena itu, sebuah aplikasi web diusulkan untuk menghilangkan peran Google Home Hub dan lebih fokus pada pelestarian privasi pengguna. Aplikasi web ini dapat digunakan untuk mengontrol, memantau, dan mengelola perangkat IoT dari berbagai merek dan perangkat, serta menyediakan fitur seperti pemantauan waktu nyata dan kontrol otomatis dari jarak jauh dengan pemicu otomatis berdasarkan peristiwa. Dengan aplikasi web ini, pengguna dapat menghubungkan perangkat IoT mereka dan mengelola izin perangkat, mengubah kata sandi perangkat, dan melihat status perangkat. Aplikasi web ini dirancang untuk berkontribusi dalam mengubah persepsi privasi pengguna saat menggunakan perangkat IoT.

Kesimpulan

Secara keseluruhan, penelitian ini berhasil mengusulkan platform User-Interface berbasis web yang efektif bagi pengguna IoT untuk memfasilitasi pengontrolan dan pengelolaan perangkat mereka dari jarak jauh dengan pemantauan data real-time untuk melindungi privasi mereka. Meskipun ada kebutuhan untuk mengintegrasikan API untuk setiap perangkat IoT, prototipe yang dibuat dapat digunakan untuk mendemonstrasikan konsep aplikasi web yang diusulkan. Hasil survei menunjukkan perlunya membuat platform di mana pengguna dapat mengontrol berbagai perangkat IoT dari jarak jauh dan situs web tersebut adalah platform yang mudah digunakan. Dengan demikian, platform tersebut dapat membantu meningkatkan persepsi pengguna tentang privasi di lingkungan IoT.

Pekerjaan Masa Depan

Pekerjaan yang disajikan di sini hanyalah prototipe untuk membuktikan konsep implementasi situs web pada manajemen perangkat IoT. Untuk penelitian dimasa depan, validasi platform yang diusulkan bisa lebih diperluas lagi dengan mempertimbangkan integrasi API untuk perangkat IoT yang bisa dikontrol dari situs web. Prototipe kayang diusulkan dalam penelitian ini masih memerlukan beberapa pekerjaan tambahan diantaranta menambahkan lebih banyak fitur seperti fitur User-Interface yang lebih umum untuk meningkatkan pengalaman pengguna. Selain itu, sistem keamanan dapat ditambahkan untuk menyediakan lebih banyak fitur, lebih banyak kategori dan perangkat IoT dapat ditambahkan serta secara paralel dengan fungsi untuk meningkatkan fungsionalitas situs web. Dengan berbagai fitur tambahan seperti kontrol suara, platform ini dapat dimodifikasi lebih luas lagi.

DAFTAR PUSTAKA

Ammar AE Elhadi, Mohd A Maarof, and Ahmed H Osman. Malware detection based on hybrid signature behaviour application programming interface call graph. American Journal of Applied Sciences, 9(3):283, 2012.

Anaconda. Anaconda software distribution version 2-2.4.0, November 2016.

Andreas Moser, Christopher Kruegel, and Engin Kirda. Limits of static analysis for malware detection. In Twenty-Third Annual Computer Security Applications Con-ference (ACSAC 2007), pages 421-430. IEEE, 2007.

Bojan Kolosnjaji, Apostolis Zarras, George Webster, and Claudia Eckert. Deep learning for classification of malware system call sequences. In Australasian Joint Conference on Artificial Intelligence, pages 137-149. Springer, 2016.

Byron P Roe, Hai-Jun Yang, Ji Zhu, Yong Liu, Ion Stancu, and Gordon McGregor. Boosted decision trees as an alternative to artificial neural networks for particle identification. Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 543(2-3):577-584, 2005.

Charles E Metz. Basic principles of roc analysis. In Seminars in nuclear medicine, volume 8, pages 283-298. Elsevier, 1978.

p-ISSN : 2808-8751 e-ISSN : 2798-2513

Christopher Manning, Prabhakar Raghavan, and Hinrich Schutze. Introduction to information retrieval. Natural Language Engineering, 16(1):100-103, 2010.

Daniel Bilar. Opcodes as predictor for malware. International Journal of Electronic Security and Digital Forensics, 1(2):156-168, 2007.

David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song, and Heng Yin. Automatically identifying trigger-based behavior in malware. In Botnet Detection, pages 65-88. Springer, 2008.

Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014.

Dilshan Keragala. Detecting malware and sandbox evasion techniques. SANS Institute InfoSec Reading Room, 16, 2016.

Fabian Pedregosa, Gael Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, et al. Scikit-learn: Machine learning in python. Journal of machine learning research, 12(Oct):2825-2830, 2011.

Francois Chollet et al. Keras. https://keras.io, 2015.

Guillaume Bonfante, Matthieu Kaczmarek, and Jean-Yves Marion. Control flow graphs as malware signatures. In International workshop on the Theory of Computer Viruses, 2007.

Guolin Ke, Qi Meng, Thomas Finley, Taifeng Wang, Wei Chen, Weidong Ma, Qiwei Ye, and Tie-Yan Liu. Lightgbm: A highly effcient gradient boosting decision tree. In Advances in Neural Information Processing Systems, pages 3146-3154, 2017.

Hamid Divandari, Bassir Pechaz, and Majid Vafaie Jahan. Malware detection using markov blanket based on opcode sequences. In 2015 International Congress on

Igor Santos, Jaime Devesa, Felix Brezo, Javier Nieves, and Pablo Garcia Bringas. Opem: A static-dynamic approach for machine-learning-based malware detection. In International Joint Conference CISIS'12-ICEUTE 12-SOCO 12 Special Sessions, pages 271-280. Springer, 2013.

J. D. Hunter. Matplotlib: A 2d graphics environment. Computing in Science & Engineering, 9(3):90-95, 2007.

Jeremy Z Kolter and Marcus A Maloof. Learning to detect malicious executables in the wild. In Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining, pages 470-478. ACM, 2004.

J-Michael Roberts. Virus share.(2011). URL https://virusshare.com, 2011.

John Nickolls, Ian Buck, and Michael Garland. Scalable parallel programming. In 2008 IEEE Hot Chips 20 Symposium (HCS), pages 40-53. IEEE, 2008.

Jon Oberheide, Michael Bailey, and Farnam Jahanian. Polypack: an automated online packing service for optimal antivirus evasion. In Proceedings of the 3rd USENIX conference on Offensive technologies, pages 9. USENIX Association, 2009.

Joshua Saxe and Konstantin Berlin. Deep neural network based malware detection using two dimensional binary program features. In 2015 10th International Conference on Malicious and Unwanted Software (MALWARE), pages 11-20. IEEE, 2015.

Karthik Raman et al. Selecting features to classify malware. InfoSec Southwest, 2012.

Katherine Heller, Krysta Svore, Angelos D Keromytis, and Salvatore Stolfo. One class support vector machines for detecting anomalous windows registry accesses. In ICDM Workshop on Data Mining for Computer Security, 2003.

Kilian Weinberger, Anirban Dasgupta, Josh Attenberg, John Langford, and Alex Smola. Feature hashing for large scale multitask learning. arXiv preprint arXiv:0902.2206, 2009.

M. Sikorski and A. Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.

Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2):6, 2012.

Martin Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. Tensor ow: A system for large-scale machine learning. In 12th fUSENIXg Symposium on Operating Systems Design and Implementation (fOSDIg 16), pages 265-283, 2016.

Michele Banko and Eric Brill. Scaling to very very large corpora for natural language disambiguation. In Proceedings of the 39th annual meeting on association for computational linguistics, pages 26-33. Association for Computational Linguistics 2001.

Mihai Christodorescu and Somesh Jha. Static analysis of executables to detect malicious patterns. Technical report, WISCONSIN UNIV-MADISON DEPT OF COMPUTER SCIENCES, 2006.

Mila Dalla Preda, Mihai Christodorescu, Somesh Jha, and Saumya Debray. A semantics-based approach to malware detection. ACM SIGPLAN Notices, 42(1):377- 388, 2007.

Naman Bagga. Measuring the effectiveness of generic malware models. Master's thesis, San Jose State University, 2017.

Philip OKane, Sakir Sezer, and Kieran McLaughlin. Obfuscation: The hidden malware. IEEE Security & Privacy, 9(5):41-47, 2011.

Randy Kath. The portable executable file format from top to bottom. MSDN Library, Microsoft Corporation, 1993.

Razvan Pascanu, Jack W Stokes, Hermineh Sanossian, Mady Marinescu, and Anil Thomas. Malware classification with recurrent networks. In 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 1916-1920. IEEE, 2015.

Rich Caruana and Alexandru Niculescu-Mizil. An empirical comparison of supervised learning algorithms. In Proceedings of the 23rd international conference on Machine learning, pages 161-168. ACM, 2006.

Robert E Schapire. The boosting approach to machine learning: An overview. In Nonlinear estimation and classification, pages 149-171. Springer, 2003.

Romain Thomas. Lief - library to instrument executable formats. https://lief.quarkslab.com/, April 2017.

Ross Quinlan. C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers, San Mateo, CA, 1993.

Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov, and Mansour Ahmadi.

Srilatha Attaluri, Scott McGhee, and Mark Stamp. Profile hidden markov models and metamorphic virus detection. Journal in computer virology, 5(2):151-169, 2009.

Stefan Van Der Walt, S Chris Colbert, and Gael Varoquaux. The numpy array: a structure for effcient numerical computation. Computing in Science & Engineering, 13(2):22, 2011.

T Jayalakshmi and A Santhakumaran. Statistical normalization and back propagation for classification. International Journal of Computer Theory and Engineering, 3(1):1793-8201, 2011.

Technology, Communication and Knowledge (ICTCK), pages 564-569. IEEE, 2015.

Tom Fawcett. An introduction to roc analysis. Pattern recognition letters, 27(8):861-874, 2006.

Travis E Oliphant. Python for scientic computing. Computing in Science & Engineering, 9(3):10-20, 2007.

Trevor Hastie, Saharon Rosset, Ji Zhu, and Hui Zou. Multi-class adaboost. Statistics and its Interface, 2(3):349-360, 2009.

p-ISSN : 2808-8751 e-ISSN : 2798-2513

Wen-Chieh Wu and Shih-Hao Hung. Droiddolphin: A dynamic android malware detection framework using big data and machine learning. In Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems, RACS '14, pages 247-252, New York, NY, USA, 2014. ACM.

Wenyi Huang and Jack W Stokes. Mtnet: a multi-task neural network for dynamic malware classification. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pages 399-418. Springer, 2016.

Wes McKinney et al. Data structures for statistical computing in python. In Proceedings of the 9th Python in Science Conference, volume 445, pages 51-56. Austin,TX, 2010.

Wikimedia Commons. Portable executable 32 bit structure in svg fixed, 2016. https://commons.wikimedia.org/wiki/File: Portable Executable 32 bit Structure in SVG fixed.svg.