JOURNAL SHIFT
VOL 2 NO 2 (2022)
ISSN 2776-8961 (ONLINE)
2808-3385 (PRINT)

Internet of Things (IoT): Security, Threats and Countermeasures

Zulkarnaim Masyhur[1*], Firmansyah Ibrahim[2] ,Didit Hermawan[3]
[1,2,3]Jurusan Sistem Informasi, Universitas Islam Negeri Alauddin Makassar, Indonesia
[1]zulkarnaim.masyhur@uin-alauddin.ac.id, [2]firmansyah.ibrahim@uin-alauddin.ac.id,
[3]didithrwn09@gmail.com

Informasi Artikel

Article historys:

Diterima Juni 23, 2022
Disetujui Juni 29, 2022
Dipublikasi Juni 30, 2022

Kata Kunci:

Internet of Things
IoT Security
IoT Data Privacy
IoT Features
Threat

ABSTRACT

Internet of Things (IoT) is a technology that is very popular lately and is starting to get busy in Indonesia, marked by various cellphone manufacturers building an IoT ecosystem. IoT can help connect objects such as sensors, vehicles, hospital instruments, household appliances and others. However, connecting these smart devices to the internet network causes various data security problems because internet technology and communication protocols have not been specifically designed to support IoT devices. The leakage of data security through the commercialization of IoT devices, causes privacy problems, threats of cyber-attacks, and organized crime. This paper aims to educate about how data security attacks in IoT and how to overcome them. To achieve this goal, we first discuss various well-known IoT reference models and define security in the context of IoT. Second, identify and classify various IoT attacks and threats. Third, described methods of countermeasures against IoT attacks. In the end, it provides some tips on securing IoT devices.

Koresponden Author:

Zulkarnaim Masyhur,
Jurusan Sistem Informasi,
Universitas Islam Negeri Alauddin Makassar,
Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia.
Email: zulkarnaim.masyhur@uin-alauddin.ac.id

1. PENDAHULUAN

Pada Tahun 1999 adalah tahun pertama kali di perkenalkannya Teknologi Internet of Things (IoT) oleh Kevin Ashton. Konsep IoT diartikan sebagai sebuah kemampuan untuk menghubungkan objek-objek cerdas dan memungkinkannya untuk berinteraksi dengan objek lain, dengan lingkungan, maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet.[1]

Internet of Things (IOT) adalah struktur di mana objek, orang disediakan dengan identitas eksklusif dan kemampuan untuk pindah data melalui jaringan tanpa memerlukan dua arah antara manusia ke manusia yaitu sumber ke tujuan atau interaksi manusia dengan komputer.

ISSN 2776-8961 (ONLINE)
2808-3385 (PRINT)

Penerapan IoT dalam perorangan sangat terasa pengaruhnya dalam kehidupan sehari – hari, seperti pada aplikasi rumah pintar dan mobil cerdas. Dari sisi penggunaan bisnis, IoT sangat berpengaruh dalam meningkatkan jumlah produksi, efisiensi, kualitas produksi, pemantauan distribusi barang, mencegah pemalsuan, mempercepat waktu ketersediaan barang pada pasar retail, manajemen rantai pasok, dan sebagainya. Dengan penerapan IoT tersebut diharapkan untuk bisa membuat kehiduapan manusia menjadi jauh lebih mudah, praktis dan nyaman. [2]

Tetapi dengan terhubungnya peranti-peranti cerdas ini ke dalam jaringan internet mengakibatkan berbagai problem keamanan data dikarenakan teknologi internet dan protokol komunikasi belum didesain secara khusus untuk mendukung perangkat IoT. Dengan bocornya kemanan data melalui komersialisasi perangkat Iot menyebabkan masalah privasi, ancaman serangan dunia maya, dan kejahatan terorganisasi. [2]

Oleh sebab itu pada paper ini akan menjelaskan dan memberikan pedoman bagi pihak – pihak pengembang dan pengguna IoT di indonesia demi peningkatan keamanan data penggunanya, dengan makalah ini juga akan membuat pembaca memahami berbagai model referensi IoT yang di kenal luas dan mendefenisikan keamananya dan yang terakhir akan diperkenalkan berbagai metode penanggulangan terhadap serangan IoT sehingga pengembang bisa mempercepat pertumbuhan IoT di indonesia dan pengguna bisa cerdas dalam menggunakan perangkat IoT.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian literature review. Penulis melakukan pencarian referensi terkait dengan keamanan privasi data. Literature review merupakan sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian dan hasil pemikiran yang sudah dihasilkan oleh para peneliti dan praktisi. Beberapa tahapan yang dilakukan dalam peneltian ini yaitu: 1) Menentukan ruang lingkup topik literature yang akan direview, dalam penelitan ini runag lingkup topiknya adalah ancaman keamanan dan metode pengamanan perangkat IoT. 2) Mengidentifikasi sumber rujukan, pada penelitian ini identifikasi dilakukan dengan melihat terbitan dari literatur yang akan direview. 3) Mereviewdan menulis review, tahap selanjutnya adalah mengambil subtansi dari setiap referensi yang dikumpulkan kemudian memberikan evaluasi dan menuliskannya kembali.

3. HASIL PENELITIAN DAN PEMBAHASAN

3.1. Internet of Things (IoT)

Internet of Thing adalah sebuah perangkat yang di konsep memiliki kemampuan untuk mentransfer data melalui jaringan internet tanpa memerlukan interaksi manusia ke manusia atau manusia dengan komputer. Cara kerja IoT dengan menggunakan sensor untuk bisa membaca dan mengumpulkan data yang dibutuhkan, Koneksi dengan menggunakan wifi atau bluetooth yang berfungsi sebagai media mengirimkan data yang telah di kumpulkan tadi oleh sensor, pengolahan data yang berfungsi mengolah data yang telah di kumpulkan sebelumnya contohnya data yang dikumpulkan lampu akan menyala otomatis pada jam 18:00 jadi setelah jam tersebut data akan diolah dan mengecek jamnya sudah benar atau tidak jika tidak lampu tidak akan menyala, dan yang terakhir adalah User Interface (UI) berfungsi sebagai tampilan yang dapat dengan mudah dipahami oleh penggunanya dalam mengelolah perangkat IoT tersebut. [1]

3.2. Implementasi Internet of Things

Sudah berbagai macam pengamplikasian IoT yang sudah di kembangkan mulai dari kehidupan sehari – hari seperti Smarthome, autonomous car, Smart farming, smart class dan sebagainya, untuk lebih jelaskan akan di jelaskan sebagai berikut

3.2.1. Smarthome

Smarthome (Rumah Pintar) adalah sebuah sistem berbantuan komputer yang akan memberikan segala kenyamanan, keselamatan, keamanan dan penghematan energi, yang berlangsung secara otomatis dan terprogram melalui komputer, pada gedung atau rumah tinggal [1]. Dapat digunakan untuk mengontrol semua peralatan dan perlengkapan yang ada

ISSN 2776-8961 (ONLINE)
2808-3385 (PRINT)

di suatu rumah dengan menggunakan suara, sensor infra merah dan kontrol jarah jauh dengan handphone.

3.2.2. Autonomous Car

Autonomous car memiliki fitur-fitur seperti GPS, kamera, computer vision, dan sensor. GPS digunakan untuk mencari rute-rute terbaik yang akan dilewati dan menghindari kepadatan jalan. GPS akan memberikan alternatif rute ketika pengguna menjumpai kemacetan Fitur kamera, sensor, dan computer vision digunakan untuk mendeteksi keadaan sekitar mobil. Dengan kamera, mobil dapat melihat kendaraan atau objek lain yang berada di sekitarnya [2]. Sehingga pengemudi bisa mengaktifkan kemudi otomatis yang dimana mobil akan jalan dengan sendirinya sesuai dengan tujuan yang sudah di masukkan ke dalam GPS tetapi untuk fitur kendali manual tidak dihilangkan agar pengemudi bisa mengontrol dengan sendiri di keadaan tertentu atau urgent.

3.2.3. Smart Farming

Smart farming adalah sistem managemen pertanian yang bertujuan untuk meningkatkan produktivitas dan penggunaan sumberdaya baik melalui peningkatan hasil atau berkurangnya input dan efek lingkungan yang merugikan dengan memanfaatkan teknologi informasi [3]. Sehingga diharapkan dengan adanya teknologi ini bisa membantu petani dalam mengelola pertaniannya

3.2.4. Smart Class

Smart Class berfungsi untuk mengontrol penggunaan fasilitas di ruangan perkuliahan, dengan menggunakan sistem yang secara otomatis dapat menyalakan dan memadamkan lampu dan AC dimana sistem tersebut dapat diatur berdasarkan waktu yang diinginkan [4]. Sehingga diharapkan dengan adanya teknologi ini pembelajaran dalam kelas bisa di laksanakan dengan efisien

3.3. Ancaman Keamanan Data pada Internet of Things (IoT)

Dengan berkembangnya teknologi Internet of Thing (IoT) tentunya juga tidak luput dari ancaman keamanan pada teknologi tersebut. IoT merupakan sistem yang sangat kompleks melibatkan berbagai komponen seperti data, komponen perangkat, sensor, dan jaringan komunikasi dan lain lain yang menyebabkan rentang terhadap berbagai ancaman seperti penyalagunaan data atau ancaman keselamatan dari penggunanya sendiri oleh sebab mari kita kenali berbagai ancaman pada Internet of Thing sebagai berikut:

3.3.1 Ancaman Keamanan IoT pada Layer Nodes

Ancaman Edge Node yaitu Peranti IoT yang menggunakan RFID readers, sensor, dan node aktuator. Serangan yang utama pada edge node ini adalah sebagai berikut.

1. Hardware Trojan. Serangan jenis hardware Trojan menyerang dengan melakukan modifikasi pada Integrated Circuit (IC) yang memungkinkan penyerang mendapatkan akses terhadap data atau perangkat lunak yang dijalankan pada IC tersebut [5]. Penyerang bisa dapat memasukkan trojan dengan cara mengubah desain IC pada saat fabrikasi atau sebelum fabrikasi dan menentukan mekanissme trigger untuk mengaktifkan trojan tersebut.

   Solusi yang dapat digunakan yaitu metode Side-Channel Analysis yaitu menyediakan pendekatan yang efektif untuk mendeteksi hardware-trojan dan firmware berbahaya yang dipasang pada perangkat IoT. mekanisme deteksi Trojan berbasis sinyal dapat dilakukan dengan membandingkan karakteristik fisik dan/atau peta distribusi panas dari IC yang mencurigakan dengan karakteristik dari IC lain yang bebas Trojan [6].
2. Non-network side-channel attack. Setiap node dapat membuka informasi sensitif pada kondisi operasi normal, bahkan ketika peranti tidak menggunakan media komunikasi nirkabel untuk transmisi data. misalnya beacon yang selalu memancarkan status peranti.

ISSN 2776-8961 (ONLINE)
2808-3385 (PRINT)

Contohnya pada perangkat IoT medis yang bisa menampilkan informasi yang bisa membuat stigma negatif bagi orang lain yang mengetahui data tersebut.

Solusi yang dapat digunakan yaitu Policy-based Mechanism and Intrusion Detection System metode berbasis kebijakan (policy) merupakan salah satu teknik yang menjanjikan untuk menyelesaikan permasalahan keamanan dan privasi pada level node ini. Pelanggaran kebijakan penting dapat dideteksi secara berkelanjutan dengan memperkenalkan Intrusion Detection System (IDS) [7].

3. Battery draining. Karena kebayakan ukuran IoT yang berukuran kecil dan baterainya juga berkapasitas kecil sehingga rawan akan serangan yang bisa mengkuras daya baterai perangkat sehingga menyebabkan gagal operasi pada perangkat IoT tersebut dalam beberapa perangkat IoT yang terkena serangan tersebut bisa membahayakan penggunanya.

   Solusi yang dapat digunakan yaitu Malicious Firmware Detection Analisis sinyal ini dapat mengungkapkan informasi berharga tentang operasi perangkat. Mirip dengan mekanisme deteksi Trojan, metode deteksi malware dapat memproses sinyal untuk mendeteksi perilaku abnormal perangkat, misalnya peningkatan konsumsi daya yang signifikan, yang merupakan hasil dari malware yang aktif pada perangkat.

3.3.2 Ancaman Keamanan pada Layer Komunikasi

Adapun untuk ancaman keamanan pada layer komunikasi biasanya memanfaatkan jaringan komunikasi untuk bisa melakukan seranngan untuk pembahasannya sebagai berikut.

1. Eavesdropping adalah serangan yang bisa mendapatkan informasi seperti username, password dan berbagai data penting lainnya. penyerang bisa mencuri data tersebut melalui kanal komunikasi perangkat IoT yang kita gunakan. Dengan data yang bocor tersebut bisa saja penyerang menyalahgunakan data atau menjualnya kepada orang lain

   Solusi yang dapat digunakan yaitu metode Kriptografi Penggunaan skema kriptografi untuk mengamankan protokol komunikasi adalah salah satu pertahanan paling efektif terhadap berbagai serangan, termasuk penyadapan dan serangan routing yang sederhana, pada layer komunikasi. Beberapa metode enkripsi telah diusulkan untuk mengatasi masalah keamanan dalam komunikasi. Teknik enkripsi-dekripsi, yang dikembangkan untuk jaringan kabel tradisional, tidak secara langsung berlaku untuk sebagian besar komponen IoT, khususnya untuk edge-node yang bertenaga baterai kecil. Edge-node biasanya berupa sensor kecil yang memiliki kapasitas baterai, daya pemrosesan, dan memori yang terbatas. Penggunaan enkripsi meningkatkan penggunaan memori, konsumsi energi, penundaan, dan kehilangan paket [8].
2. Side Channel Attack Serangan jenis ini merupakan serangan yang kuat terhadap enkripsi, walaupun relatif sulit untuk diimplementasikan. Serangan jenis ini biasanya termasuk noninvasif. Penyerang biasanya hanya mengekstrak informasi yang tanpa sengaja bocor. Misalnya, informasi tentang jarak antar paket yang berurutan, pita frekuensi, dan modulasi yang digunakan. Salah satu ciri serangan ini adalah tidak mudah terdeteksi sehingga akan lebih sulit untuk menghindarinya.

   Solusi yang dapat digunakan yaitu De-patterning dan decentralization merupakan dua metode utama yang diusulkan untuk memberikan anonimitas dan pertahanan terhadap sidechannel attack. Selalu ada trade-off antara anonimitas dan kebutuhan untuk berbagi informasi. Pengacakan pola transmisi data dapat melindungi sistem dari serangan side-channel, misalnya dengan menyisipkan paket tambahan yang dapat mengubah pola trafik sehingga pola yang terbentuk tidak dapat dikenali. Metode alternatif untuk memastikan

ISSN 2776-8961 (ONLINE)
2808-3385 (PRINT)

anonimitas adalah distribusi data sensitif melalui spanning tree sehingga tidak ada node yang memiliki tampilan lengkap dari data asli. Metode ini disebut desentralisasi [9].

3.3.3 Ancaman Keamanan pada Edge Computing

Ancaman keamanan yang biasanya menyerang pada komponen layer 3 pada IoT walaupun keamanan ini belum terlalu banyak dieksplorasi. Berikut beberapa ancaman yang bisa terjadi pad edge computing

1. Malicious Injection yaitu validasi masukan (input) yang tidak memadai memungkinkan datangnya serangan berupa injeksi masukan berbahaya. Penyerang menyuntikkan inputan yang menyebabkan penyedia layanan menjalankan suatu perintah (aktivitas) atas nama penyerang. contohnya, penyerang memasukkan komponen yang tidak sesuai ke salah satu level di bawah computing node ini (level komunikasi atau edge node) yang mampu menyuntikkan masukan berbahaya ke server. Setelah itu, penyerang dapat mencuri data, mengganggu integritas basis data, atau memotong autentikasi. Pesan kesalahan basis data standar yang ditampilkan oleh server basis data juga dapat dimanfaatkan penyerang. Dalam situasi ketika penyerang tidak memiliki pengetahuan tentang tabel basis data, penyerang dapat dengan sengaja membuat skrip yang dapat membangkitkan exception untuk mengungkapkan rincian lebih lanjut tentang setiap tabel dan nama-nama kolomnya [10].
   Solusi yang dapat digunakan yaitu Pre-Testing Pengujian terhadap proses pembaruan dan implementasi desain penting untuk dilakukan sebelum desain tersebut digunakan dalam sistem IoT. Perilaku seluruh sistem dan komponennya, seperti router, edge-node, dan server, harus diperiksa dengan teliti dengan memasukkan masukan yang berbeda ke sistem dan memantau keluaran. Secara khusus, upaya prapengujian dilakukan untuk mengidentifikasi kemungkinan skenario serangan dan menyimulasikan skenario ini untuk melihat cara sistem merespons [11].
2. Integrity Attack Against Machine Learning dua jenis serangan dapat diluncurkan terhadap metode machine learning yang digunakan dalam sistem IoT, yaitu kausatif dan eksplorasi. Dalam serangan kausatif, penyerang mengubah proses pelatihan dengan memanipulasi dataset pelatihan, sedangkan dalam serangan eksplorasi, penyerang mengeksploitasi kerentanan tanpa mengubah proses pelatihan. Penelitian barubaru ini telah memperkenalkan jenis baru serangan kausatif, yang disebut poisoning attack [12], Motivasi utamanya adalah untuk menyebabkan algoritme klasifikasi menyimpang dari pembelajaran model yang valid dengan memanipulasi dataset.
   Solusi yang dapat digunakan yaitu Outlier Detection: Tujuan pertahanan keamanan terhadap serangan integritas data pada metode machine learning adalah untuk mengurangi pengaruh penambahan data invalid terhadap hasil. Data invalid ini merupakan outlier (penyimpangan) pada dataset yang digunakan. Sebuah framework untuk pertahanan terhadap serangan jenis poisoning telah dikembangkan berdasarkan statistik untuk mengurangi efek keracunan [13].

4. KESIMPULAN

Seiring dengan berkembangnya teknologi IoT menimbulkan beberapa ancaman keamanan yang memungkinkan dieksploitasi oleh orang-orang yang tidak bertanggung jawab. Diharapkan melalui jurnal ini, pembaca dapat mengetahui berbagai ancaman keamanan dan metode pengamanan yang dapat digunakan. Sehingga ketika memanfaatkan teknologi IoT dapat lebih menyadari berbagai ancaman dan kerentanan sehingga dapat lebih bijak dalam menggunakan perangkat IoT.

DAFTAR PUSTAKA

[1] M. E. M.Dwisnanto Putro, ST., "Perancangan Shading Device pada Smart home," *E-Journal Tek. Elektro Dan Komput.*, vol. 3, no. 5, pp. 49–54, 2014.

[2] A. Setyo and P. T. Prasetyaningrum, "Perancangan Aplikasi Internet of Thing (IoT) Autonomous Pada Mobil Designing Car Autonomous Internet of Thing (IoT) Application," no. 84, pp. 35–38, 2018.

[3] A. Balafoutis *et al.*, "Precision agriculture technologies positively contributing to ghg emissions mitigation, farm productivity and economics," *Sustain.*, vol. 9, no. 8, pp. 1–28, 2017, doi: 10.3390/su9081339.

[4] T. Aisyah, Y. R. Roshadi, and A. Setiawan, "Prototipe Kelas Pintar (Smart Class) dengan Memanfaatkan Teknologi IoT The Protoype of Smart Class using IoT Technology," no. November 2020, pp. 83–92.

[5] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, 2017, doi: 10.1109/TETC.2016.2606384.

[6] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware trojan detection using thermal and power maps," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 33, no. 12, 2014, doi: 10.1109/TCAD.2014.2354293.

[7] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Secur. Distrib. Grid, Mobile, Pervasive Comput.*, pp. 367–409, 2007, doi: 10.1201/9780849379253-20.

[8] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," 2017, doi: 10.1109/I-SMAC.2017.8058307.

[9] R. Kumar and S. Rajalakshmi, "Mobile sensor cloud computing: Controlling and securing data processing over smart environment through Mobile Sensor Cloud Computing (MSCC)," 2013, doi: 10.1109/CSA.2013.166.

[10] S. W. Boyd and A. D. Keromytis, "SQLrand: Preventing SQL injection attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3089, 2004, doi: 10.1007/978-3-540-24852-1_21.

[11] H. Mouratidis and P. Giorgini, "Security Attack Testing (SAT)-testing the security of information systems at design time," *Inf. Syst.*, vol. 32, no. 8, 2007, doi: 10.1016/j.is.2007.03.002.

[12] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," in *Proceedings of the 29th International Conference on Machine Learning, ICML 2012*, 2012, vol. 2.

[13] B. I. P. Rubinstein *et al.*, "Antidote: Understanding and defending against poisoning of anomaly detectors," 2009, doi: 10.1145/1644893.1644895.