Vol. 6 No. 1 Juni 2025 Hal : 245 - 255 E-ISSN: 2723-1089
P-ISSN: 2776-7779

Studi Literatur Keamanan Data Dalam Sistem Smart Home Berbasis IoT

Jodi Putra Aljabbar[1], M. Rifaldy Febriansyah Rajaguguk[2],Novan Wijaya[3]
Sistem Informasi , Fakultas Ilmu Komputer dan Rekayasa ,
Universitas Multi Data Palembang , Kota Palembang
*Coresponding Email: jodiptra@gmail.com, rifaldif888@gmail.com , novan.wijaya@mdp.ac.id

Abstrak

Sistem *smart home* berbasis Internet of Things (IoT) semakin populer karena kemampuannya dalam meningkatkan kenyamanan dan efisiensi rumah tangga. Namun, adopsi teknologi ini menghadirkan tantangan signifikan terkait keamanan data. Penelitian ini bertujuan untuk mengkaji berbagai potensi ancaman keamanan serta solusi mitigasinya dalam sistem *smart home* berbasis IoT. Metode yang digunakan adalah studi literatur terhadap jurnal dan laporan teknis terbaru. Hasil kajian menunjukkan bahwa serangan seperti *sniffing*, *spoofing*, dan *unauthorized access* merupakan ancaman umum dalam ekosistem IoT. Strategi seperti enkripsi end-to-end, autentikasi kuat, serta pembaruan perangkat lunak secara berkala direkomendasikan untuk meminimalkan risiko. Penelitian ini memberikan wawasan awal bagi pengembang dan pengguna sistem *smart home* dalam upaya meningkatkan keamanan data.

Kata Kunci: Keamanan data, Internet of Things, Smart home, Enkripsi, Autentikasi

Abstract

Internet of Things (IoT)-based smart home systems are gaining popularity due to their ability to improve household comfort and efficiency. However, the adoption of this technology presents significant challenges related to data security. This study aims to examine various potential security threats and their mitigation solutions in IoT-based smart home systems. The method used is a literature study of the latest journals and technical reports. The results of the study indicate that attacks such as sniffing, spoofing, and unauthorized access are common threats in the IoT ecosystem. Strategies such as end-to-end encryption, strong authentication, and regular software updates are recommended to minimize risks. This study provides initial insights for developers and users of smart home systems in an effort to improve data security.

Keywords: Data security, Internet of Things, Smart home, Encryption, Authentication

PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) telah mendorong lahirnya berbagai inovasi, salah satunya adalah sistem smart home. Sistem ini mengintegrasikan perangkat-perangkat elektronik dalam rumah seperti lampu,

kamera, sensor suhu, dan pintu otomatis ke dalam satu sistem yang dapat dikontrol melalui jaringan internet. Dengan adanya otomatisasi ini, pengguna dapat meningkatkan kenyamanan, efisiensi energi, dan keamanan lingkungan rumah (Mutiha dkk., 2023).

Namun, di balik kemudahan yang ditawarkan, sistem smart home menyimpan tantangan besar, khususnya dalam aspek keamanan data. Data yang dihasilkan dan ditransmisikan oleh perangkat IoT bersifat pribadi dan sensitif, sehingga rentan terhadap penyadapan, pencurian data, dan penyalahgunaan oleh pihak tidak bertanggung jawab (Prasetyo Eka Putra dkk., 2023). Hal ini diperparah dengan fakta bahwa banyak perangkat IoT masih belum menerapkan protokol keamanan yang memadai, seperti enkripsi data dan autentikasi ganda (Sijabat dkk., 2025).

Permasalahan utama yang dihadapi dalam implementasi sistem smart home adalah lemahnya pengamanan terhadap data pengguna. Serangan seperti sniffing, spoofing, dan unauthorized access menjadi ancaman nyata dalam ekosistem ini. Kurangnya kesadaran pengguna akan pentingnya keamanan data serta minimnya regulasi yang mengatur keamanan IoT juga turut memperbesar risiko (Khatib Sulaiman dkk., t.t.).

Berbagai studi terdahulu telah mencoba mengevaluasi risiko dan celah keamanan dalam sistem smart home dari berbagai pendekatan. Misalnya, analisis terhadap keamanan jaringan berbasis simulasi menunjukkan bahwa kelemahan dapat terletak pada arsitektur dasar jaringan IoT itu sendiri (Laksamana, 2019). Sementara itu, pendekatan penetration testing mampu mengungkap celah keamanan yang tidak terdeteksi dalam pengujian konvensional (Gunawan, t.t.). Tidak kalah penting, perlindungan data pribadi juga perlu didukung oleh kerangka hukum yang memadai agar pengguna merasa aman dalam menggunakan layanan berbasis IoT (Dewi Rosadi & Gumelar Pratama, 2018).

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan studi literatur terhadap berbagai publikasi ilmiah yang membahas keamanan data dalam sistem smart home berbasis IoT. Fokus kajian difokuskan pada jenis-jenis ancaman yang umum terjadi serta strategi mitigasi yang direkomendasikan oleh para peneliti. Diharapkan hasil dari penelitian ini dapat memberikan gambaran awal bagi pengembang dan pengguna dalam membangun sistem smart home yang aman dan andal.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (literature review). Subjek dalam penelitian ini adalah berbagai dokumen ilmiah berupa artikel jurnal nasional berbahasa Indonesia yang membahas topik keamanan data pada sistem smart home berbasis Internet of Things (IoT).

Pengumpulan data dilakukan melalui penelusuran artikel dari berbagai sumber seperti portal jurnal nasional terakreditasi, repositori institusi pendidikan tinggi, dan situs jurnal ilmiah terbuka seperti GARUDA, Neliti, dan Google Scholar. Kriteria inklusi dalam pemilihan artikel adalah: (1) artikel ditulis dalam Bahasa Indonesia, (2) terbit dalam kurun waktu 5 tahun terakhir, dan (3) membahas secara langsung isu keamanan data atau ancaman siber dalam sistem smart home atau IoT.

Sebanyak 10 artikel yang memenuhi kriteria telah dipilih untuk di analisis, termasuk artikel oleh (Sutarjo & Waluyo, 2024),(Ratna Sari, 2024) dan (Cahyaaty dkk., 2024) yang membahas topik keamanan IoT secara mendalam dalam konteks Indonesia. Instrumen penelitian berupa tabel klasifikasi untuk mencatat informasi dari setiap artikel, seperti judul, penulis, tahun terbit, jenis ancaman keamanan yang dibahas, serta rekomendasi solusi atau mitigasi yang ditawarkan. Teknik analisis data yang digunakan adalah analisis konten (content analysis), dengan cara mengelompokkan temuan-temuan dari masing-masing literatur ke dalam tema-

tema utama, seperti jenis ancaman keamanan, kelemahan sistem, dan metode perlindungan data.

Metode ini digunakan untuk memperoleh pemahaman menyeluruh mengenai tren ancaman keamanan yang umum terjadi pada sistem smart home, serta strategi mitigasi yang disarankan oleh para peneliti di Indonesia. Pendekatan ini relevan untuk menjawab tujuan penelitian yang bersifat eksploratif dan deskriptif.

TABEL SINSTESIS LITERATUR

No	Judul Artikel	Penulis	Tahun	Jenis Ancaman Keamanan	Rekomendasi Solusi / Mitigasi
1.	Analisis Keamanan Pada Sistem Internet of Things Untuk Pengendalian Perangkat Elektronik Rumah Tangga	Mutiha, Siagian, Siregar, & Siahaan	2023	Akses tidak sah, penyadapan data, dan lemahnya enkripsi komunikasi antar perangkat.	Implementasi umum IoT dalam smart home
2.	Privasi dan Keamanan Penerapan IoT Dalam	Prasetyo Eka Putra, Mellyana	2023	Kebocoran data, akses tidak sah	Enkripsi, manajemen identitas, firewall

	Kehidupan Sehari-Hari: Tantangan dan Implikasi	Dewi, & Hamzah			
3.	Perlindungan Data Pribadi dalam Era IoT: Studi Kasus Kebocoran Data Lion Air	Sijabat	2024	Kebocoran data besar (studi kasus)	Audit keamanan, regulasi perlindungan data pribadi
4.	Evaluasi Kerentanan Keamanan Pada Perangkat IoT: Studi Kasus Pada Smart Home	Khatib Sulaiman, Cahyo Utomo, Kholisotul, & Rojak	2022	Sniffing, spoofing, unauthorized access	Enkripsi E2E, autentikasi kuat, update berkala
5.	Analisis Keamanan Jaringan dalam Smart Home IoT Menggunakan	Fahrizal Satya Laksamana	2019	Kerentanan jaringan	Identifikasi kerentanan, prioritas keamanan jaringan

	Cisco Packet Tracer				
6.	Uji Kerentanan Jaringan Perangkat IoT pada Smart Home Menggunakan Metode Penetration Testing	Hari Saeni Gunawan	2024	Brute force, sniffing, MITM	Pengujian penetrasi, simulasi serangan
7.	Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia	Dewi Rosadi & Pratama	2018	Pelanggaran privasi, kurangnya regulasi	Instrumen hukum, perlindungan data pribadi
8.	Implementasi Kriptografi AES-128 Untuk Pengamanan Data Purchase Order Pada PT	Sutarjo & Waluyo	2024	Penyadapan data,akses tidak sah	Enkripsi AES,Autentikasi Token

	Antilope Madju Puri Indah				
9.	Analisis Keamanan Sistem Informasi dalam Era Internet Of Things(IoT)	Ratna Sari	2024	DoS, spoofing, sniffing	Firewall, segmentasi jaringan
10.	Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi	Cahyaaty dkk.	2024	Unauthorized access, eksploitasi hak akses	Audit log, manajemen akses

HASIL DAN PEMBAHASAN

Berdasarkan studi literatur terhadap sejumlah jurnal dan dokumen teknis terkini, ditemukan bahwa sistem smart home berbasis IoT memiliki beberapa tantangan signifikan dalam hal keamanan data. Serangan yang paling umum ditemukan dalam sistem ini meliputi:

1. **Sniffing**

   Teknik penyadapan data yang lewat di jaringan. Hal ini dapat terjadi karena banyak perangkat IoT tidak mengenkripsi data mereka secara memadai, sehingga data sensitive dapat diakses oleh pihak yang tidak berwenang.

2. **Spoofing**

   Serangan di mana pelaku menyamar sebagai perangkat sah dalam jaringan, untuk mengakses sistem atau menyampaikan perintah palsu. Spoofing sering berhasil karena lemahnya mekanisme autentikasi dalam banyak perangkat IoT.

3. **Unauthorized Access**

   Akses ilegal oleh pihak yang tidak sah ke sistem smart home. Hal ini disebabkan oleh pengguna menggunakan kata sandi lemah, atau perangkat tidak mendukung autentikasi dua faktor.

Faktor Penyebab Kerentanan

a) Banyak perangkat IoT diproduksi dengan keamanan minimum untuk menekan biaya produksi.

b) Kurangnya kesadaran pengguna tentang pentingnya pengamanan dan pembaruan sistem.

c) Minimnya standar keamanan yang berlaku secara universal untuk produk IoT.

Strategi Mitigasi

Dari berbagai sumber literatur, ditemukan beberapa strategi mitigasi yang direkomendasikan oleh para peneliti:

a) **Enkripsi End-to-End (E2E:** Untuk menjamin bahwa data hanya dapat dibaca oleh pengirim dan penerima yang sah. Standar seperti AES-256 disarankan untuk digunakan.

b) **Autentikasi Kuat:** Termasuk penggunaan password yang kompleks, autentikasi dua faktor (2FA), dan sertifikat digital.

c) **Pembaruan Perangkat Lunak Berkala:** Produsen perlu menyediakan pembaruan firmware untuk menambal celah keamanan yang ditemukan dari waktu ke waktu.

d) **Segmentasi Jaringan:** Memisahkan jaringan IoT dari jaringan utama rumah dapat mencegah penyebaran serangan dari satu perangkat ke perangkat lain.

e) **Manajemen Akses yang Baik:** Menggunakan sistem pengendalian hak akses dan log aktivitas agar aktivitas mencurigakan dapat dilacak lebih cepat.

Selain strategi-strategi di atas, Pentingnya penggunaan enkripsi AES dan autentikasi berbasis token sebagai langkah penting dalam mengamankan komunikasi antar perangkat IoT (Sutarjo & Waluyo, 2024). Dan efektivitas segmentasi jaringan dan penggunaan firewall dalam mencegah serangan seperti DoS dan spoofing (Ratna Sari, 2024). Setelah itu pentingnya audit log dan sistem manajemen hak akses untuk mendeteksi serta mencegah penyalahgunaan akses yang mencurigakan pada sistem smart home (Cahyaaty dkk., 2024).

Diskusi

Hasil temuan ini sejalan dengan penelitian sebelumnya yang juga menyatakan bahwa kelemahan utama dari sistem smart home adalah aspek keamanan data (Ahmed dkk., 2020). Hal ini menunjukkan bahwa pengembangan teknologi IoT yang pesat belum diimbangi dengan peningkatan sistem keamanan yang mumpuni.

Dengan demikian, meskipun IoT menawarkan kenyamanan, efisiensi energi, dan otomatisasi, aspek keamanan data harus dijadikan prioritas utama, terutama karena sistem ini mengakses data sensitif pengguna. Penelitian ini menekankan

pentingnya peran pengembang, regulator, dan pengguna dalam membangun ekosistem smart home yang aman.

SIMPULAN

Penelitian ini menyimpulkan bahwa sistem smart home berbasis *Internet of Things* (IoT) menghadapi tantangan serius dalam aspek keamanan data, terutama terhadap serangan seperti *sniffing, spoofing*, dan akses tidak sah. Berdasarkan hasil studi literatur, kerentanan tersebut sebagian besar disebabkan oleh lemahnya protokol keamanan bawaan perangkat IoT, kurangnya kesadaran pengguna terhadap risiko siber, serta belum optimalnya pembaruan perangkat lunak secara berkala. Untuk mengatasi hal ini, berbagai strategi mitigasi telah direkomendasikan oleh para peneliti, antara lain penerapan enkripsi *end-to-end*, *autentikasi* yang kuat seperti *multi-factor authentication*, serta pemisahan jaringan untuk menghindari eskalasi serangan. Dengan memahami pola ancaman dan solusi yang tersedia, pengembang dan pengguna smart home dapat mengambil langkah preventif yang tepat guna meningkatkan keamanan dan keandalan sistem. Penelitian ini diharapkan dapat menjadi dasar untuk riset lanjutan maupun pengembangan kebijakan keamanan yang lebih komprehensif pada ekosistem IoT di masa mendatang.

DAFTAR PUSTAKA

Ahmed, A. J., Sadeeq, M. A. M., Abdulla, A. I., Abdulraheem, A. S., Salih, A. A., Ahmed, A. J., Ferzor, B. M., Salih, O., & Mohammed, I. (2020). *Internet of Things and Smart Home Security* (Vol. 62). https://www.researchgate.net/publication/350313736

Cahyaaty, T. A., Wijaya, I., Dafin, M., Dzky, A., Prasojo, H. G., & Prakoso, S. H. (2024). Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce Shopee Terhadap Ancaman Data Pribadi. *Journal of Information and Information Security (JIFORTY)*, *5*(2), 133–144. http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). URGENSI PERLINDUNGANDATA PRIVASIDALAM ERA EKONOMI DIGITAL DI INDONESIA. *Veritas et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/vej.2916

Gunawan, H. S. (t.t.). *Uji Kerentanan Jaringan Perangkat Internet of Things (IoT) pada Smart-Home Menggunakan Penerapan Metode Penetration*.

Khatib Sulaiman, J., Cahyo Utomo, I., Kholisotul, N., Muhammad Izudin Rojak, K., & Artikel Abstrak, I. (t.t.). Evaluasi Kerentanan Keamanan Pada Perangkat IoT: Studi Kasus Pada Smart Home. *Indonesian Journal of Computer Science*.

Laksamana, F. S. (2019). *ANALISIS KEAMANAN JARINGAN DALAM SMARTHOME INTERNET OF THINGS (IoT) MENGGUNAKAN CISCO PACKET TRACER DENGAN METODE SQUARE*.

Mutiha, E., Siagian, P., Siregar, J., & Siahaan, R. H. (2023). ANALISIS KEAMANAN PADA SISTEM INTERNET OF THINGS UNTUK PENGENDALIAN PERANGKAT ELEKTRONIK RUMAH TANGGA. *Jurnal Teknologi Informasi dan Industri*, *4*(1).

Prasetyo Eka Putra, F., Mellyana Dewi, S., & Hamzah, A. (2023). *Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi*. *5*(2). https://doi.org/10.37034/jsisfotek.v5i1.232

Ratna Sari, D. (2024). Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT). *Technologia Journal: Jurnal Informatika*, *1*(2), 3046–9163. https://doi.org/10.62872/v2tffe44

Sijabat, J. Y., Hukum, F., Sosial, I., Hukum, J., & Kewarganegaraan, D. (2025). *Perlindungan Data Pribadi dalam Era Internet of Things (Studi Kasus Kebocoran Data Lion Air)*. *2*, 44–49. https://doi.org/10.62383/humif.v2i2.1457

Sutarjo, H., & Waluyo, S. (2024). *IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK PENGAMANAN DATA PURCHASE ORDER PADA PT ANTILOPE MADJU PURI INDAH* (Vol. 3, Nomor 2).