https://jurnal.pustakagalerimandiri.co.id/index.php/pustakadata
DOI: https://doi.org/10.55382/jurnalpustakadata.v6i1.1554

Jurnal Pustaka Data

Pusat Akses Kajian Database, Analisa Teknologi, dan Arsitektur Komputer

Vol. 6 No. 1 (2026) 11– 15

E ISSN: 2809-7483

Perancangan Model Keamanan Komunikasi IoT–Web Server Berbasis HTTP Request dan JWT

Asep Marzuki[1], Bobi Handoko[2], Abdul Zaky[3], Dedy Yasriady[4], Ahmad Fauzan Azim[5]
[1,3,4] Informatika, Fakultas Teknologi Kreatif dan Ekonomi, Universitas Awal Bros
[2] Administrasi Rumah Sakit, Fakultas Ilmu Kesehatan, Universitas Awal Bros
[5]Teknik Komputer, Fakultas Vokasi, Institut Azzuhra
[1]kangasep.net@gmail.com, [2]bobihandoko.bh@gmail.com, [3]zakimathua@gmail.com, [4]yasriady@gmail.com, [5]ahmadfauzanazim20@gmail.com

Abstract

The main problem in developing Internet of Things (IoT)-based systems lies in data security during communication between IoT devices and web servers. Smart systems that exchange transaction data and user identities require secure integration mechanisms to prevent information misuse. Weaknesses in data communication can potentially lead to various security threats, such as man-in-the-middle attacks, identity theft, and transaction data manipulation. This study proposes the design of an HTTP Request-based communication security model equipped with an authentication mechanism using JSON Web Token (JWT). JWT was chosen because it is lightweight, suitable for IoT devices with limited resources, and capable of ensuring data integrity through the use of digital signatures. This approach allows every data exchange between IoT devices and servers to be securely validated, thereby minimizing the risk of data leaks and alterations. The research methods included analyzing security requirements for IoT–server communication, designing a security model architecture based on JSON Web Token (JWT), and evaluating the model through latency analysis and authentication success rates based on the designed communication scenarios. This research successfully designed and analyzed an HTTP Request-based IoT–web server communication security model with a JSON Web Token (JWT) authentication mechanism. The test results showed that the use of JWT with a valid secret key was able to provide effective access control, as indicated by the successful authentication and validation of data communication between IoT devices and servers.

Keywords: security model, Internet of Things, HTTP request, JSON Web Token, web server

Abstrak

Permasalahan utama dalam pengembangan sistem berbasis Internet of Things (IoT) terletak pada aspek keamanan data selama proses komunikasi antara perangkat IoT dan web server. Sistem pintar yang melakukan pertukaran data transaksi dan identitas pengguna memerlukan mekanisme integrasi yang aman agar informasi tidak disalahgunakan. Kelemahan pada komunikasi data berpotensi menimbulkan berbagai ancaman keamanan, seperti serangan man-in-the-middle, pencurian identitas, serta manipulasi data transaksi. Penelitian ini mengusulkan perancangan model keamanan komunikasi berbasis HTTP Request yang dilengkapi mekanisme autentikasi menggunakan JSON Web Token (JWT). JWT dipilih karena bersifat ringan, sesuai untuk perangkat IoT dengan keterbatasan sumber daya, serta mampu menjamin integritas data melalui penggunaan tanda tangan digital. Pendekatan ini memungkinkan setiap pertukaran data antara perangkat IoT dan server tervalidasi secara aman, sehingga risiko kebocoran dan perubahan data dapat diminimalkan. Metode penelitian meliputi analisis kebutuhan keamanan pada komunikasi IoT–server, perancangan arsitektur model keamanan berbasis JSON Web Token (JWT), serta evaluasi model melalui analisis latensi dan tingkat keberhasilan autentikasi berdasarkan skenario komunikasi yang dirancang. Penelitian ini berhasil merancang dan menganalisis model keamanan komunikasi IoT–web server berbasis HTTP Request dengan mekanisme autentikasi JSON Web Token (JWT). Hasil pengujian

Submitted : 17-12-2025 | Reviewed : 18-01-2026 | Accepted : 06-02-2026

menunjukkan bahwa penggunaan JWT dengan secret key yang valid mampu memberikan kontrol akses yang efektif, ditandai dengan keberhasilan autentikasi dan validasi komunikasi data antara perangkat IoT dan server.

Kata kunci: model keamanan, internet of things, http request, JSON web token, webserver

1. Pendahuluan

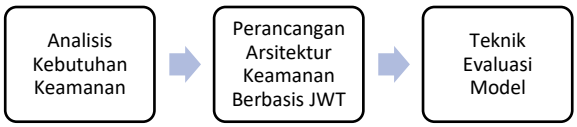
Perkembangan Internet of Things (IoT) mendorong meningkatnya pemanfaatan perangkat pintar yang terhubung dengan web server untuk melakukan pertukaran data secara real time[1]. Integrasi ini banyak digunakan pada sistem yang melibatkan transaksi data, identitas pengguna, dan pengambilan keputusan berbasis server. Namun, komunikasi data antara perangkat IoT dan web server masih menghadapi tantangan serius pada aspek keamanan, khususnya pada mekanisme autentikasi dan integritas data yang dikirimkan melalui jaringan terbuka[2].

Keterbatasan sumber daya pada perangkat IoT sering kali menyebabkan penerapan mekanisme keamanan yang kurang optimal, sehingga membuka celah terhadap berbagai ancaman keamanan. Beberapa penelitian sebelumnya telah membahas pengamanan komunikasi IoT menggunakan berbagai pendekatan, seperti penggunaan API key statis, enkripsi berbasis TLS[3], maupun token autentikasi sederhana. Pendekatan tersebut umumnya mampu meningkatkan keamanan komunikasi, namun masih memiliki keterbatasan, antara lain tingginya overhead komputasi, manajemen kredensial yang kompleks, serta kurangnya mekanisme validasi integritas data yang efisien untuk perangkat dengan sumber daya terbatas[4].

Penelitian lain mulai mengadopsi JSON Web Token (JWT) sebagai mekanisme autentikasi [5], [6]karena sifatnya yang ringan dan stateless, tetapi sebagian besar masih berfokus pada implementasi aplikasi web atau sistem berskala besar, tanpa membahas perancangan model arsitektur keamanan yang spesifik untuk komunikasi IoT–server. Berdasarkan kondisi tersebut, terdapat celah penelitian pada kebutuhan akan model keamanan komunikasi IoT–web server yang ringan, terstruktur, dan sesuai dengan karakteristik perangkat IoT [7]. Diperlukan sebuah pendekatan yang tidak hanya berfokus pada mekanisme autentikasi, tetapi juga pada perancangan arsitektur komunikasi yang mampu menjamin validitas dan integritas data secara efisien [7]. Oleh karena itu, penelitian ini diarahkan untuk merancang model keamanan komunikasi IoT–server berbasis HTTP Request dengan mekanisme autentikasi menggunakan JSON Web Token [8].

2. Metode Penelitian

Penelitian ini menggunakan metode analisis dan perancangan arsitektur keamanan komunikasi IoT–web server berbasis HTTP Request dengan autentikasi JSON Web Token (JWT). Tahapan penelitian difokuskan pada perancangan model keamanan dan evaluasi skenario komunikasi tanpa melibatkan implementasi perangkat keras secara langsung seperti pada gambar 1.



Gambar 1. Metode Penelitian

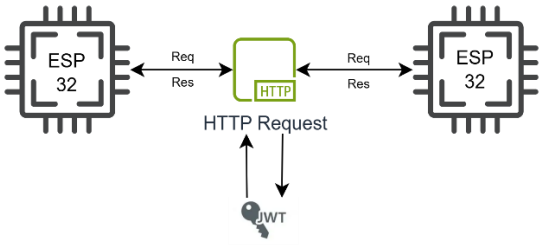
2.1. Analisis Kebutuhan Keamanan

Analisis kebutuhan dilakukan dengan mengidentifikasi titik pertukaran data antara perangkat IoT dan web server pada skenario komunikasi berbasis HTTP. Parameter keamanan yang dianalisis meliputi mekanisme autentikasi, validasi identitas perangkat, serta integritas data selama transmisi [9]. Analisis ancaman difokuskan pada potensi serangan man-in-the-middle, pemalsuan identitas perangkat, dan manipulasi payload data. Perangkat yang digunakan dalam pengujian yaitu mikro kontroller ESP32 yang dikomunikasikan dalam satu jaringan[10]. Hasil analisis ini digunakan sebagai dasar dalam penentuan kebutuhan token, struktur klaim JWT, dan alur autentikasi.

2.2 Perancangan Arsitektur Keamanan Berbasis JWT

Perancangan arsitektur dilakukan dengan mendefinisikan alur komunikasi IoT–server yang terdiri dari proses permintaan token, penyertaan token pada setiap HTTP request, serta proses verifikasi token di sisi server. JWT dirancang menggunakan algoritma tanda tangan digital berbasis HMAC dengan panjang token rata-rata ±200–300 byte untuk menjaga efisiensi transmisi data [8], [11], [12]. Struktur klaim token mencakup identitas perangkat, waktu kedaluwarsa (expiration time), dan penanda akses layanan. Setiap request tervalidasi melalui proses verifikasi signature dan waktu berlaku token sebelum data diproses oleh server. Model arsitektur sistem keamanan berbasis JWT seperti pada gambar 2.

Submitted : 17-12-2025 | Reviewed : 18-01-2026 | Accepted : 06-02-2026



Gambar 2. Arsitektur Sistem Keamanan Berbasis JWT

2.2 Teknik Evaluasi Model

Evaluasi model dilakukan melalui pengujian skenario komunikasi yang dirancang secara berulang sebanyak tiga kali replikasi untuk setiap skenario autentikasi. Parameter evaluasi meliputi waktu respons autentikasi (latensi) yang diukur dalam satuan milidetik serta tingkat keberhasilan validasi token pada setiap request. Pengukuran dilakukan pada kondisi jaringan yang sama untuk menjaga konsistensi hasil. Metode autentikasi dan validasi JWT yang digunakan mengacu pada teknik yang telah mapan dan dirujuk dari penelitian sebelumnya.

Metode yang digunakan pada penelitian ini dirancang agar dapat direproduksi dengan mengikuti tahapan analisis, perancangan arsitektur, serta skenario evaluasi komunikasi IoT–server berbasis JWT sebagaimana dijelaskan pada setiap tahap.

2.3 Kode Program

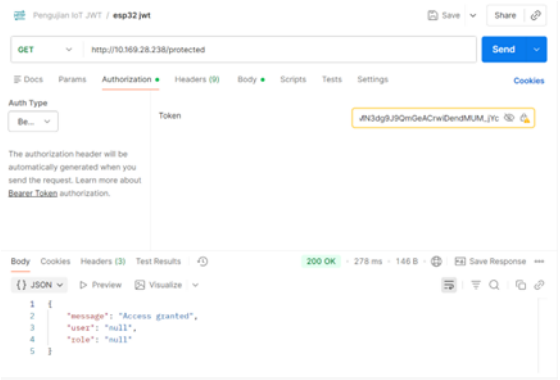
Program Enkripsi HMAC SHA256

```
// Fungsi HMAC SHA256
    String hmacSha256(String data, String key) {
        unsigned char hmacResult[32];
        mbedtls_md_context_t ctx;
        mbedtls_md_type_t md_type =
    MBEDTLS_MD_SHA256;
        mbedtls_md_init(&ctx);
        mbedtls_md_setup(&ctx,
    mbedtls_md_info_from_type(md_type), 1);
        mbedtls_md_hmac_starts(&ctx, (const unsigned
    char*)key.c_str(), key.length());
        mbedtls_md_hmac_update(&ctx, (const unsigned
    char*)data.c_str(), data.length());
        mbedtls_md_hmac_finish(&ctx, hmacResult);
        mbedtls_md_free(&ctx);

        String base64 = "";
        const char* base64_chars =
    "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmno
    pqrstuvwxyz0123456789-_";
        for (int i = 0; i < 32; i += 3) {
          int b1 = hmacResult[i];
          int b2 = i + 1 < 32 ? hmacResult[i + 1] : 0;
          int b3 = i + 2 < 32 ? hmacResult[i + 2] : 0;
          base64 += base64_chars[b1 >> 2];
          base64 += base64_chars[((b1 & 0x3) << 4) | (b2 >>
    4)];
          if (i + 1 < 32)
            base64 += base64_chars[((b2 & 0xF) << 2) | (b3 >>
    6)];
          if (i + 2 < 32)
            base64 += base64_chars[b3 & 0x3F];
        }
        return base64;
    }
```

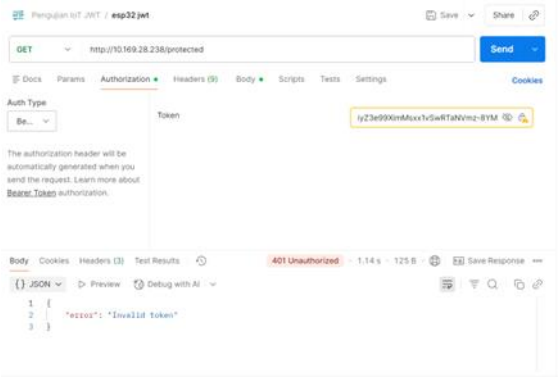
3. Hasil dan Pembahasan

Hasil pengujian menunjukkan bahwa penggunaan mekanisme keamanan JSON Web Token (JWT) berpengaruh terhadap proses autentikasi dan waktu respons komunikasi antara perangkat IoT dan web server. Pengujian menggunakan JWT dengan secret key yang valid berhasil mengakses endpoint API dengan status success dan menghasilkan latensi sebesar 278 ms. Hal ini menunjukkan bahwa mekanisme verifikasi token berjalan dengan baik[9] dan mampu memvalidasi identitas perangkat secara tepat. Pengujian Rest API dengan valid token seperti pada gambar 3.



Gambar 3. Pengujian Rest API dengan Valid Token

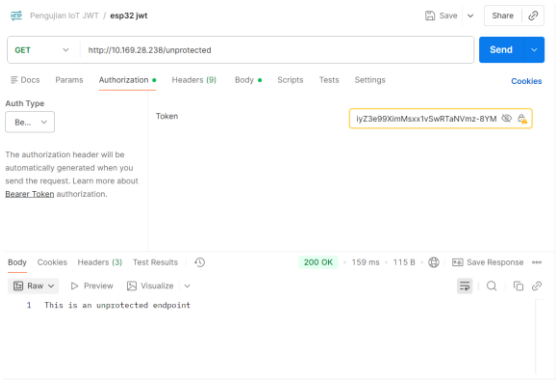
Sebaliknya, pada pengujian JWT dengan secret key yang tidak valid, akses ke endpoint API ditolak dengan status unauthorized. Latensi yang dihasilkan meningkat hingga 1,1 detik, yang disebabkan oleh proses verifikasi token yang gagal sebelum permintaan dihentikan oleh sistem keamanan. Hasil ini menegaskan efektivitas JWT dalam mencegah akses tidak sah ke layanan server. Gambar 4 adalah tampilan pengujian rest API dengan invalid token.



Gambar 4. Pengujian Rest API dengan Invalid Token

Pengujian tanpa penerapan mekanisme keamanan JWT menunjukkan latensi paling rendah, yaitu 159 ms, dengan status akses success. Meskipun memberikan waktu respons yang lebih cepat, kondisi

ini tidak menyediakan mekanisme autentikasi dan validasi identitas perangkat. Dengan demikian, penerapan JWT menambah overhead latensi, namun memberikan peningkatan signifikan pada aspek keamanan komunikasi IoT–server. Seperti tampak pada gambar 5.



Gambar 5. Pengujian Rest API tanpa keamanan JWT

Tabel 1. Hasil perbandingan pengujian Rest API

Skenario Pengujian	Mekanisme Keamanan	Validitas Secret Key	Status Akses	Latensi
Akses endpoint dengan JWT	JSON Web Token (JWT)	Benar	Success	278 ms
Akses endpoint dengan JWT	JSON Web Token (JWT)	Salah	Unauthorized	1.1 s
Akses endpoint tanpa JWT	Tanpa autentikasi	–	Success	159 ms

Hasil pengujian seperti pada tabel 1 menunjukkan bahwa penerapan model keamanan berbasis JSON Web Token (JWT) mampu mengendalikan akses komunikasi antara perangkat IoT dan web server secara efektif. Pada skenario penggunaan JWT dengan secret key yang valid, permintaan berhasil diproses dengan status success dan latensi sebesar 278 ms. Hasil ini mengindikasikan bahwa mekanisme autentikasi dan verifikasi token dapat dijalankan dengan baik pada komunikasi berbasis HTTP [5], sekaligus memastikan bahwa hanya perangkat terautentikasi yang dapat mengakses endpoint API .

Sebaliknya, pada pengujian menggunakan JWT dengan secret key yang tidak valid, sistem secara konsisten menolak akses dengan status unauthorized. Peningkatan latensi hingga 1,1 detik menunjukkan adanya proses verifikasi token yang gagal sebelum permintaan dihentikan oleh server. Kondisi ini memperlihatkan bahwa model keamanan yang dirancang mampu mendeteksi ketidaksesuaian kredensial dan mencegah akses tidak sah, meskipun dengan konsekuensi waktu respons yang lebih tinggi akibat proses validasi tambahan.

Pengujian tanpa penerapan JWT menghasilkan latensi paling rendah, yaitu 159 ms, dengan status akses success. Meskipun kinerja waktu respons lebih baik, skenario ini tidak menyediakan mekanisme autentikasi maupun validasi identitas perangkat. Temuan ini menegaskan adanya trade-off antara performa dan keamanan, di mana penerapan JWT menambah overhead latensi namun memberikan peningkatan signifikan pada aspek keamanan komunikasi.

Secara umum, hasil pengujian menjawab pertanyaan penelitian bahwa model keamanan komunikasi IoT–web server berbasis JWT mampu meningkatkan kontrol akses dan integritas komunikasi dibandingkan skenario tanpa mekanisme keamanan[7], [12]. Meskipun terdapat peningkatan latensi, nilainya masih berada dalam batas yang dapat diterima untuk komunikasi IoT berbasis HTTP. Hasil ini dapat digeneralisasikan pada sistem IoT lain yang memerlukan autentikasi ringan dan stateless, dengan catatan bahwa optimasi lebih lanjut dapat dilakukan untuk menekan latensi pada proses verifikasi token.

4. Kesimpulan

Penelitian ini berhasil merancang dan menganalisis model keamanan komunikasi IoT–web server berbasis HTTP Request dengan mekanisme autentikasi JSON Web Token (JWT). Hasil pengujian menunjukkan bahwa penggunaan JWT dengan secret key yang valid mampu memberikan kontrol akses yang efektif, ditandai dengan keberhasilan autentikasi dan validasi komunikasi data antara perangkat IoT dan server.

Model keamanan yang diusulkan terbukti mampu menolak akses tidak sah secara konsisten ketika secret key tidak valid, sehingga menunjukkan efektivitas JWT dalam mencegah penyalahgunaan akses dan manipulasi data. Meskipun penerapan JWT menimbulkan peningkatan latensi dibandingkan komunikasi tanpa mekanisme keamanan, nilai latensi yang dihasilkan masih berada dalam batas yang dapat diterima untuk sistem IoT berbasis HTTP.

Secara keseluruhan, model keamanan berbasis JWT ini dapat digeneralisasikan untuk berbagai sistem IoT yang memerlukan mekanisme autentikasi ringan, stateless, dan mudah diintegrasikan dengan web server. Penelitian selanjutnya dapat diarahkan pada optimasi proses verifikasi token dan evaluasi pada skala sistem yang lebih besar untuk meningkatkan performa tanpa mengurangi tingkat keamanan.

Ucapan Terimakasih

Ucapan Terimakasih Kepada Universitas Awal Bros yang telah memberikan pendanaan melalui skema pendanaan hibah perguruan tinggi dan kepada Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM) Universitas Awal Bros yang

telah menyelenggarakan program hibah perguruan tinggi.

Daftar Rujukan

[1] A. Marzuki and A. C. Adha, "Prototype Alat Pendeteksi Banjir Berbasis Internet of Thing Terintegrasi Aplikasi Instant Messanging," vol. 5, no. 2, pp. 1–6, 2024.

[2] Singh, P., Kumar, R., & Sharma, M., "Enhancing IoT Communication Security through Lightweight Token Mechanisms," J. Netw. Comput. Appl., 2021.

[3] B. Baharuddin, H. Wakkang, and B. Irianto, "Implementasi Web Service Dengan Metode Rest Api Untuk Integrasi Data Covid 19 Di Sulawesi Selatan," J. Sintaks Log., vol. 2, no. 1, pp. 236–241, 2022, doi: 10.31850/jsilog.v2i1.1035.

[4] A. Fernandes, E., Jung, J., & Prakash, "Security Analysis of Emerging Smart Home Applications," IEEE Symp. Secur. Priv., pp. 395–420, 2017.

[5] Park, J., & Kim, H., "Performance Analysis of JWT for Secure IoT Communication," J. Inf. Process. Syst., pp. 943–955, 2019.

[6] S. J. S. Lee, "Vulnerabilities and Encryption Applications of JWT-Based Authentication Methods," vol. 10, 2025.

[7] N. Hong, M. Kim, M. Jun, and J. Kang, "A Study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment," 2017, doi: 10.3390/su9071099.

[8] A. Warda, P. Putra, A. Bhawiyuga, and M. Data, "Implementasi Autentikasi JSON Web Token (JWT) Sebagai Mekanisme Autentikasi Protokol MQTT Pada Perangkat NodeMCU," vol. 2, no. 2, pp. 584–593, 2018.

[9] S. Ahmed and Q. Mahmood, "An authentication based scheme for applications using JSON web token," in 2019 22nd International Multitopic Conference (INMIC), 2019, pp. 1–6. doi: 10.1109/INMIC48123.2019.9022766.

[10] T. Aditya Firmansah and K. Eko Susilo, "Techno Xplore Jurnal Ilmu Komputer dan Teknologi Informasi Prototype Sistem Monitoring dan Kontroling Banjir Berbasis Internet of Things Menggunakan ESP32," 2020.

[11] S. Dalimunthe, J. Reza, and A. Marzuki, "THE MODEL FOR STORING TOKENS IN LOCAL STORAGE (COOKIES) USING JSON WEB TOKEN (JWT) WITH HMAC (HASH-BASED MESSAGE AUTHENTICATION CODE) IN E-LEARNING SYSTEMS," vol. 3, no. 2, pp. 149–155, 2022.

[12] M. R. Hosenkhan and B. K. Pattanayak, "A Framework for Secure Communication on Internet of Things (IoT)," in Progress in Advanced Computing and Intelligent Engineering, C. R. Panigrahi, B. Pati, B. K. Pattanayak, S. Amic, and K.-C. Li, Eds., Singapore: Springer Singapore, 2021, pp. 599–605.

Submitted : 17-12-2025 | Reviewed : 18-01-2026 | Accepted : 06-02-2026