

# PERANCANGAN KEAMANAN SISTEM *MONITORING SMART HYDROPONIC* FIK UPNVJ MENGGUNAKAN JSON WEB TOKEN (JWT)

ADINDA RIZKI SYA'BANA DIVA

## ABSTRAK

Sistem *monitoring smart hydroponic* FIK UPNVJ yang berbasis *website* dengan akses terbuka memiliki kerentanan pada mekanisme akses kontrol, khususnya karena lemahnya standarisasi keamanan pada perangkat IoT dan keterbatasan autentikasi berbasis sesi yang bersifat *stateful* dalam lingkungan terdistribusi. Penelitian ini bertujuan merancang dan mengimplementasikan arsitektur keamanan akses kontrol berbasis JSON Web Token (JWT) pada sistem tersebut, serta menguji keefisienannya dari segi keamanan dan penggunaan sumber daya dibandingkan autentikasi berbasis sesi. Sistem dibangun di atas *stack* FastAPI, Vue.js, PostgreSQL/TimescaleDB, dan Docker dengan dua lingkungan independen untuk masing-masing skema. Pengujian keamanan dilakukan menggunakan *script* bash Kali Linux terhadap 14 *endpoint restricted* dengan 4 skenario serangan untuk masing-masing skema, sedangkan pengujian performa menggunakan Locust dengan 50 pengguna virtual selama 60 detik sebanyak 500 kali percobaan. Hasil pengujian menunjukkan JWT mencapai *success rate* 100%, sementara sesi hanya 78,57% akibat kegagalan pada skenario *session replay attack* dan *session timeout*. Dari segi performa, JWT mencatat *response time* 368,31 ms dan *throughput* 35,16 req/s, sedikit lebih baik dibandingkan sesi (370,61 ms; 35,10 req/s), serta penggunaan memori lebih rendah (463,86 berbanding 468,88 MB), sementara penggunaan CPU kedua skema relatif setara (0,50% berbanding 0,51%). Penelitian ini menyimpulkan bahwa JWT dengan algoritma ECDSA (ES256) lebih unggul secara keamanan dengan tingkat risiko yang jauh lebih rendah serta performa yang setara, sehingga direkomendasikan sebagai mekanisme akses kontrol optimal pada sistem *monitoring smart hydroponic* FIK UPNVJ.

Kata kunci: akses kontrol, autentikasi, IoT, JSON Web Token, keamanan sistem.

# SECURITY DESIGN OF THE FIK UPNVJ SMART HYDROPONIC MONITORING SYSTEM USING JSON WEB TOKEN (JWT)

ADINDA RIZKI SYA'BANA DIVA

## ABSTRACT

*The FIK UPNVJ smart hydroponic monitoring system, built as a publicly accessible web-based platform, has vulnerabilities in its access control mechanism, particularly due to weak security standardization in IoT devices and the limitations of stateful session-based authentication in distributed environments. This research aims to design and implement a JWT-based access control security architecture for the system, as well as to evaluate its efficiency in terms of security and resource utilization compared to session-based authentication. The system was built on a FastAPI, Vue.js, PostgreSQL/TimescaleDB, and Docker stack, with two independent environments for each scheme. Security testing was conducted using Kali Linux bash scripts against 14 restricted endpoints with 4 attack scenarios for each scheme, while performance testing used Locust with 50 virtual users over 60 seconds across 500 trials. The results show that JWT achieved a 100% success rate, while session-based authentication reached only 78.57% due to failures in the session replay attack and session timeout scenarios. In terms of performance, JWT recorded a response time of 368.31 ms and a throughput of 35.16 req/s, slightly better than session (370.61 ms; 35.10 req/s), along with lower memory usage (463.86 compared to 468.88 MB), while CPU usage between the two schemes was relatively equal (0.50% compared to 0.51%). This study concludes that JWT with the ECDSA (ES256) algorithm is superior in terms of security, with a significantly lower risk level, and comparable performance, and is therefore recommended as the optimal access control mechanism for the FIK UPNVJ smart hydroponic monitoring system.*

*Keywords: access control, authentication, IoT, JSON Web Token, system security.*