BAB 5. PENUTUP

5.1. Kesimpulan

Berdasarkan analisis sistem *monitoring smart hydroponic* yang sudah ada, perancangan kembali sistem dengan metode keamanan, pengujian keamanan dan performa yang berfokus pada penggunaan autentikasi JWT yang diusulkan di awal, hingga pada hasil penelitian yang dilakukan, dapat ditarik kesimpulan sebagai berikut:

1. Perancangan dan implementasi arsitektur keamanan akses kontrol berbasis JWT pada sistem *monitoring smart hydroponic* FIK UPNVJ berhasil dilakukan dengan meredesain sistem eksisting yang sebelumnya tidak memiliki mekanisme autentikasi yang memadai. Sistem yang dibangun mengintegrasikan dua skema keamanan akses kontrol secara independen, yaitu *session baseline* dan JWT berbasis algoritma ECDSA (ES256), di atas *stack* FastAPI, Vue.js, PostgreSQL/TimescaleDB, dan Docker dengan konfigurasi *database* dan lingkungan *container* yang terpisah. Arsitektur JWT yang diimplementasikan mencakup validasi tanda tangan kriptografi asimetris pada setiap *request* ke *endpoint restricted*, mekanisme pencabutan token berbasis token_version di basis data sebagai pengganti *stateful blacklist*, serta penerapan RBAC yang membatasi hak akses berdasarkan peran pengguna (*user*, *admin*, dan *superadmin*) secara konsisten di seluruh lapisan sistem.
2. Pengujian keefisienan JWT dalam mengamankan akses kontrol dari segi keamanan dan penggunaan sumber daya menunjukkan bahwa JWT lebih unggul dibandingkan dengan autentikasi berbasis *session* pada kedua aspek yang diuji. Dari segi keamanan, JWT mencapai *success rate* sebesar 100% pada 14 pengujian terhadap 4 skenario serangan, meliputi kredensial tidak valid, manipulasi *signature* token, modifikasi *payload*, *token replay attack*, dan validasi *expiry time*, di mana seluruh percobaan serangan berhasil ditolak dengan respons HTTP 401 yang tepat, sementara autentikasi *session* hanya mencapai *success rate* 78,57% akibat kegagalan pada skenario *session replay attack* dan *session timeout*. Dari segi efisiensi penggunaan sumber daya berdasarkan rata-rata 500 kali percobaan, JWT mencatat *response time* sebesar 368,31 ms dan *throughput* 35,16 req/s, sedikit lebih baik dibandingkan *session* sebesar 370,61 ms dan 35,10 req/s, serta konsumsi memori yang lebih rendah dengan rata-rata 463,86 MB dibandingkan *session* sebesar 468,88 MB (selisih 5,02 MB), sedangkan penggunaan CPU kedua skema relatif setara dengan selisih yang tidak signifikan sebesar 0,01% (*session* 0,50%, JWT 0,51%). Dengan demikian, dari segi keamanan JWT memiliki tingkat risiko yang jauh lebih rendah, dan dari segi penggunaan sumber daya JWT juga lebih efisien dibandingkan *session*, sehingga JWT dapat direkomendasikan sebagai

mekanisme autentikasi yang efisien dan aman untuk diterapkan pada sistem *monitoring smart hydroponic* FIK UPNVJ, khususnya dalam mendukung karakteristik sistem IoT yang terdistribusi dan membutuhkan efisiensi penggunaan sumber daya.

5.2. Saran

Berdasarkan hasil penelitian, peneliti mengusulkan beberapa saran untuk pengembangan dan penelitian selanjutnya terkait perancangan keamanan sistem *monitoring* dalam penerapan di lingkungan IoT, antara lain:

1. Perluasan cakupan skenario pengujian keamanan tidak terbatas pada pengujian keamanan skenario berbasis akses kontrol dan autentikasi saja. Melainkan lebih bervariatif dan lebih komprehensif seperti serangan *SQL Injection*, *Cross-Site Scripting* (XSS), *Man-in-the-Middle* (MitM), serta pengujian terhadap lapisan komunikasi MQTT pada perangkat sensor IoT itu sendiri, sehingga diperoleh gambaran keamanan sistem yang lebih menyeluruh.
2. Menerapkan algoritma kriptografi ECDSA yang lebih spesifik dan pengujian *algorithm confusion attack* dengan mengeksplorasi perbandingan varian kurva eliptik lain seperti ES384 (P-384) atau ES512 (P-521), sekaligus menguji ketahanan sistem terhadap serangan *algorithm confusion* seperti *downgrade* dari ECDSA ke HMAC sebagai skenario pengujian keamanan yang lebih spesifik terhadap arsitektur JWT.
3. Pengujian performa pada skala beban yang lebih besar dan lingkungan yang lebih realistis yaitu menguji sistem dengan jumlah pengguna yang lebih besar (misalnya 200–500 *concurrent users*) serta pada lingkungan infrastruktur yang lebih mendekati produksi, seperti lingkungan *cloud* atau *load balancer* terdistribusi, untuk memvalidasi keunggulan sifat *stateless* JWT dalam skenario *horizontal scaling*.