STUDI KOMPARASI KINERJA DAN KEAMANAN *JSON WEB TOKEN (JWT)* DAN *PLATFORM AGNOSTIC SECURITY TOKENS (PASETO)* PADA *RESTful API* APLIKASI PASAR MURAH

Disusun Oleh :

Ejah Said Mansur

22206051012

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGRI SUNAN KALIJAGA

YOGYAKARTA

2025

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1945/Un.02/DST/PP.00.9/08/2025

Tugas Akhir dengan judul : STUDI KOMPARASI KINERJA DAN KEAMANAN JSON WEB TOKEN (JWT) DAN PLATFORM AGNOSTIC SECURITY TOKENS (PASETO) PADA RESTful API APLIKASI PASAR MURAH

yang dipersiapkan dan disusun oleh:

Nama	: EJAH SAID MANSUR, S.Kom
Nomor Induk Mahasiswa	: 22206051012
Telah diujikan pada	: Jumat, 08 Agustus 2025
Nilai ujian Tugas Akhir	: A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 68a4da3119277

Penguji I

Ir. Maria Ulfah Siregar, S.Kom., MIT., Ph.D.
SIGNED

Valid ID: 68a7b9c21a60a

Penguji II

Dr. Ir. Sumarsono, S.T., M.Kom.
SIGNED

Valid ID: 68a82d584b38f

Yogyakarta, 08 Agustus 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 68a8a5dadf504

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Ejah Said Mansur

NIM : 22206051012

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwa naskah tesis ini secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yag dirujuk sumbernya.

Yogyakarta, Agustus 2025

Saya yang menyatakan,

EJAH SAID MANSUR

NIM: 22206051012

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama : Ejah Said Mansur

NIM : 22206051012

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwa naskah tesis ini secara keseluruhan benar-benar bebas dari plagiasi. Jika di kemudian hari terbukti melakukan plagiasi, maka saya siap ditindak sesuai ketentuan hukum yang berlaku.

Yogyakarta, Agustus 2025

Saya yang menyatakan,

EJAH SAID MANSUR

NIM: 22206051012

NOTA DINAS PEMBIMBING

Yth,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
Yogyakarta

Assalamu'alaikum Wr. Wb,

Setelah melakukan bimbingan, arahan dan koreksi terhadap penulisan tesis yang berjudul:

STUDI KOMPARASI KINERJA DAN KEAMANAN JSON WEB TOKEN (JWT) DAN PLATFORM AGNOSTIC SECURITY TOKENS (PASETO) PADA RESTful API APLIKASI PASAR MURAH

Yang ditulis oleh:

Nama	: Ejah Said Mansur
NIM	: 22206051012
Jenjang	: Magister
Program Studi	: Informatika

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Program Studi Magister Informatika UIN Sunan Kalijaga Yogyakarta untuk diujikan dalam rangka memperoleh gelar Magister Informatika.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, Agustus 2025

Pembimbing,

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.

ABSTRACT

Authentication is a crucial aspect in maintaining the security of user data within a system. This study aims to compare two authentication protocols, JSON Web Token (JWT) and Platform Agnostic Security Tokens (PASETO), implemented on the RESTful API of the Pasar Murah Application. The research method uses a quantitative approach by conducting performance and security testing for each protocol. The test results show that JWT has better performance than PASETO. The average token generation time for JWT is recorded at 1.68 ms, while PASETO requires 2.35 ms. The token transfer time for JWT is 31.62 ms, while PASETO takes 35.94 ms. In terms of size, the JWT token is 809 bytes, whereas the PASETO token is slightly larger at 839 bytes. However, in terms of security, PASETO demonstrates greater strength. Based on the security testing results, the JWT token is considered secure against several types of attacks listed in the Top 3 OWASP API Security 2023, such as Broken Authentication, Broken Object Level Authorization , Broken Object Property Level Authorization. However, JWT remains vulnerable to Broken User Authentication threats. In contrast, PASETO shows stronger resistance, successfully withstanding all three types of attacks without exposing any vulnerabilities.

***Keywords**: RESTful, API, JWT, PASETO*

ABSTRAK

Otentikasi merupakan aspek penting dalam menjaga keamanan data pengguna pada suatu sistem. Penelitian ini bertujuan untuk membandingkan dua protokol JSON Web Token (JWT) dan Platform Agnostic Security Tokens (PASETO), yang diimplementasikan pada RESTful API Aplikasi Pasar Murah. Metode penelitian menggunakan pendekatan kuantitatif dengan melakukan pengujian performa dan keamanan masing-masing protokol. Hasil pengujian menunjukkan bahwa JWT memiliki kinerja lebih unggul dibandingkan PASETO. Rata-rata waktu pembuatan token JWT tercatat sebesar 1,68 ms, sedangkan PASETO sebesar 2,35 ms. Waktu transfer token JWT adalah 31,62 ms, sedangkan PASETO membutuhkan waktu 35,94 ms. Dari segi ukuran, token JWT berukuran 809 byte, sementara token PASETO sedikit lebih besar, yaitu 839 byte. Namun, dari aspek keamanan, PASETO menunjukkan keunggulan yang lebih baik. Berdasarkan hasil pengujian keamanan, token JWT dinyatakan aman terhadap beberapa jenis serangan yang dikategorikan dalam Top 3 OWASP API Security 2023, seperti *Broken Authentication, Broken Object Level Authorization , Broken Object Property Level Authorization.* Namun, JWT masih rentan terhadap ancaman Broken User Authentication. Sebaliknya, token PASETO menunjukkan ketahanan yang lebih baik karena berhasil lolos dari ketiga jenis serangan tersebut tanpa menunjukkan kerentanan.

Kata Kunci: *RESTful, API, JWT, PASETO*.

KATA PENGANTAR

Assalamualaikum wr.wb.

Puji syukur penulis panjatkan ke hadirat ALLAH SWT, yang telah melimpahkan rahmat, hidayah, dan pertolongan-Nya kepada penulis sehingga Tesis ini dapat terselesaikan dengan baik. Tesis dengan judul "Studi Komparasi Kinerja Dan Keamanan JSON Web Token (JWT) Dan Platform Agnostic Security Tokens (PASETO) Pada Restful API Aplikasi Pasar Murah" ini diajukan untuk memenuhi sebagian persyaratan guna memperoleh gelar Magister Progam Magister Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta. Penulis menyadari bahwa keberhasilan ini tidak terlepas dari bantuan dari bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Kedua orang tua Bapak Zenal Arifin dan Ibu Robiah beserta keluarga.
2. Istri tercinta Siti Nurjamjam, S.Pd, M.A
3. Bapak Prof. Noorhaidi Hasan, S.Ag., M.A., M.Phil., Ph.D. Selaku Rektor pada UIN Sunan Kalijaga Yogyakarta yang telah memberikan kesempatan menempuh studi ini.
4. Ibu Dr. Dra Hj. Khurul Wardati, M.Si. selaku Dekan Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta yang juga telah memberikan kesempatan untuk menempuh pendidikan di Fakultas Sains dan Teknologi UIN Snan Kalijaga Yogyakarta.
5. Bapak Dr. Ir. Sumarsono, S.T., M.Kom. selaku Kepala Prodi Informatika S2 UIN Sunan Kalijaga Yogyakarta yang telah membantu penulis selama menempuh pendidikan.

6. Bapak Dr. Bambang Sugiantoro, S.Si., M.T. selaku pembimbing yang telah berkenan merelakan waktu, tenaga, dan ilmunya guna memberikan bimbingan kepada penulis dalam menyelesaikan Tesis ini, serta ucapan terima kasih dan penghargaan yang setinggi-tingginya, yang dengan penuh kesabaran dan kearifan telah memberikan bimbingan, arahan, dan dorongan di sela-sela kesibukanya.
7. Ibu Ir. Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Dosen Penasehat Akademik yang telah berkenan membimbing dari proses awal perkuliahan sampai akhir saat ini.
8. Bapak dan Ibu Dosen, TU dan tenaga lain Prodi Informatika S2 UIN Sunan Kalijaga Yogyakarta, khususnya yang memberi kuliah, yang telah memberikan banyak ilmu pengetahuan sehingga penulis dapat melaksanakan penelitian dan menyusun hasil penelitian tersebut menjadi Tesis ini.
9. Keluarga besar Pondok Pesantren Al-Hikmah Mugarsari dan Madrasah Aliyah Plus Keterampilan Al-Hikmah Kota Tasikmalaya yang telah mendukung saya menempuh pendidikan di UIN Sunan Kalijaga Yogyakarta.
10. Teman-teman mahasiswa Prodi Informatika S2 UIN Sunan Kalijaga Yogyakarta yang telah memberikan dukungan dalam penulisan Tesis ini.
11. Teman jauh saya Ihsan Hasanudin yang telah memberikan dukungan dan bimbingan dalam penelitian tesis ini.
12. Ucapan terima kasih juga saya sampaikan kepada semua pihak yang tidak mungkin saya sebutkan satu demi satu, yang telah

banyak memberikan bantuan dan dukungan selama penyusunan Tesis ini.

Semoga Allah SWT senantiasa melimpahkan rahmat dan hidayah-Nya kepada kita semua. Penulis berharap semoga Tesis ini dapat bermanfaat bagi penulis khususnya dan pembaca pada umumnya.

Wassalamu'alaikum wr. wb.

Yogyakarta, Agustus 2025

Penyusun

Ejah Said Mansur

NIM. 22206051012

HALAMAN PERSEMBAHAN

Tesis ini penulis mempersembahkan untuk:

Almamater Tercinta

Prodi Informatika S2

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sunan Kalijaga Yogyakarta

MOTTO

Bertumbuh Dalam Senyap

(Ejah Said Mansur)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam era digital saat ini, keamanan data dan informasi menjadi salah satu aspek yang sangat penting, terutama dalam pengembangan aplikasi berbasis web. *RESTful API* (*Representational State Transfer Application Programming Interface*) telah menjadi standar dalam komunikasi antara *client* dan *server* (Nurchasanah & Palasara, 2025). *RESTful API* yang digunakan dalam suatu sistem harus dipastikan mengunakan keamanan dalam proses otentikasi dan otorisasi sitem tersebut. Keamanan *RESTful API* bertujuan untuk mengamankan jalur komunikasi data, melindungi kerahasiaan dan integritas data, serta menggunakan otentikasi untuk membatasi akses pengguna (Anugrah & Fakhruddin, 2020). Hal yang paling penting pada sistem *RESTful API* adalah proses otentikasi dan otorisasi karena keduanya berperan sebagai inti keamanan dalam mengakses sumber daya.

Otentikasi merupakan suatu proses verifikasi yang menentukan apakah seseorang berhak mengakses suatu sistem maupun tidak, sedangkan otorisasi adalah suatu proses penentuan hak akses kepada seseorang. Contoh sederhana adalah proses otentikasi dan otorisasi adalah proses *login* pada suatu sistem, ketika seorang *user* akan masuk kedalam sistem, selanjutnya *user* tersebut akan di verifikasi dan divalidasi oleh sistem, apakah *credential* tersebut *valid* atau tidak, jika *credential* milik user tersebut *valid,* maka user berhak mengakses ke dalam sistem tersebut. Berbagai metode otentikasi dan otorisasi

digunakan, di antaranya adalah *token-based authentication, Basic Authentication* dengan *username* dan *password*, *Session-Based Authentication* menggunakan session ID, *API Key Authentication* dengan kunci unik, *OAuth* 2.0 untuk *login* melalui pihak ketiga, serta Mutual TLS (mTLS) yang memakai sertifikat digital.

Setiap metode memiliki tingkat keamanan dan kegunaan berbeda sesuai kebutuhan sistem. Namun, metode otentikasi dan otoriasi yang saat ini banyak digunakan adalah *Token-based authentication*. Metode *Token-based authentication* banyak digunakan karena menawarkan keamanan, fleksibilitas, dan skalabilitas yang lebih baik dibanding metode lain. Dengan menggunakan token, server tidak perlu menyimpan session di sisi server sehingga sistem lebih ringan dan cocok untuk aplikasi berskala besar. Token juga bersifat *stateless*, artinya dapat digunakan di berbagai platform (web, mobile, IoT) tanpa ketergantungan pada server tertentu. Selain itu, token biasanya memiliki masa berlaku (*expiry time*) sehingga lebih aman, serta bisa memuat informasi tambahan (*claims*) yang memudahkan proses otorisasi. Pada pengembangan *RESTful API* modern token yang umum digunakan untuk prosen otentikasi dan otoriasai adalah *JSON Web Token* (JWT) (et al., 2023), kemudian alternatif lain Adalah dengan menggunakan *Platform Agnostic Security Tokens* (PASETO) (Maulana Awangga et al., 2024).

JSON Web Token (JWT) merupakan token string *JSON* yang berguna untuk sistem otentikasi dan pertukaran informasi (Putra et al., 2018). JWT memungkinkan pengguna untuk memilih algoritma mana yang akan digunakan dalam implementasinya. Algoritma penandatanganan yang disediakan oleh JWT adalah RSA, ECDSA,

dan HMAC. Algoritma tersebut merupakan salah satu algoritma enkripsi yang paling unggul dan efisien, ketika diimplementasikan pada arsitektur JWT (Rahmatulloh et al., 2018). Implementasi *JWT* dalam keamanan sistem adalah untuk menanggulangi serta mengembangkan sistem yang dapat mencegah pengulangan otentifikasi (Mestre et al., 2018).

Selain JWT, terdapat otentikasi berbasis token yang disebut *Platform-Agnostic Security Tokens* (PASETO) yang bisa melakukan enkripsi pada proses otentikasi suatu sistem. Algoritma yang diterapkan dalam token PASETO ini hanya dapat diakses dan diketahui oleh server PASETO. Hal ini bertujuan untuk mencegah penyerang mengetahui algoritma yang digunakan sehingga mengurangi terjadinya pemalsuan token. Token PASETO hanya menyediakan versi protokol sendiri (Arciszewski, 2017). Dibandingkan dengan JWT yang memungkinkan pengguna untuk memilih algoritma apa saja yang digunakan, PASETO mengarahkan pengguna untuk menggunakan versi protokol yang sudah menyertakan algoritma milik PASETO sendiri.

Parameter kinerja pada suatu token umumnya meliputi pembuatan token, waktu transfer token, dan ukuran token yang dihasilkan. Proses pembuatan token harus efisien agar tidak membebani server ketika banyak pengguna melakukan login secara bersamaan. Waktu transfer token juga menjadi aspek penting karena token dikirim pada setiap permintaan, sehingga semakin cepat proses pengiriman dan validasinya, semakin baik kinerja sistem. Selain itu, ukuran token yang dihasilkan perlu diperhatikan, sebab token yang terlalu besar dapat memperlambat komunikasi antara klien dan server,

terutama pada jaringan dengan *bandwidth* terbatas. Dengan mengoptimalkan ketiga parameter tersebut, sistem dapat mencapai keseimbangan antara keamanan, kecepatan, dan efisiensi dalam otentikasi berbasis token.

Selain pada parameter kinerja, hal yang harus diperhatikan adalah keamanan token, terutama dalam pengembangan sistem berbasis *RESTful API* yang mengacu pada parameter *OWASP API* Security. Token harus dilindungi dari potensi kebocoran, misalnya dengan penyimpanan yang aman di sisi klien, penggunaan protokol HTTPS untuk mencegah penyadapan, serta penerapan masa berlaku (*expiry time*) dan mekanisme *refresh* token agar tidak disalahgunakan. OWASP API juga menekankan pentingnya mitigasi terhadap serangan umum seperti *broken authentication, broken object level authorization* dan serangan lain. Oleh karena itu, selain mengoptimalkan kinerja, pengembang perlu memastikan bahwa token dikelola dengan standar keamanan tinggi agar *RESTful API* tetap terlindungi dari ancaman yang dapat mengganggu integritas dan keamanan sistem.

Beberapa penelitian telah membahas otentikasi berbasis token, khususnya *JSON Web Token* (JWT) dan PASETO. Pada penelitian (Gunawan & Rahmatulloh, 2019) dan (Mansur et al., 2023) mengimplementasikan token JWT pada sistem Arsitektur berbasis *RESTful API*, namun pada penelitian tersebut tidak dilakukan pengujian token. Kemudian penelitian lain yang dilakukan (Darmawan et al., 2021), implementasi JWT dengan algoritma HMAC-SHA256 melakukan pengujian keamanan dengan teknik CSRF pada penyimpanan cookie, namun belum dilakukan

perbandingan kinerja dan keamanan token, penelitian ini hanya terbatas pada JWT dengan algoritma HMAC-SHA256. Penelitian (Rahmatulloh et al., 2018) (Series & Science, 2019) meneliti kinerja JWT dengan parameter waktu pembuatan, ukuran, dan waktu transfer menggunakan algoritma RSA, ECDSA, dan HMAC. Sedangkan penelitian pada token PASETO (Sitorus et al., 2020), melakukan pengujian keamanan PASETO versi v2.l dan v2.p dengan Parameter encode/decode Base65, eksploitasi algoritma none, dan eksploitasi algoritma simetris-asimetris.

Kemudian penelitian terkait perbandingan kinerja dan keamanan token JWT dan PASETO sudah pernah dilakukan (Nugraha et al., 2023) dengan parameter algoritma yang digunakan HMAC-SHA384 untuk JWT dan protokol V3 dengan algoritma AES-256-CTR + HMAC-SHA384 untuk PASETO kemudian implementasi pembangunan RESTful API. Hasil yang didapatkan menunjukan JWT lebih baik dalam hal kecepatan ,transfer token serta ukuran yang dihasilkan lebih sedikit menyita penyimpanan. Namun perkembangan token terus berkembang, menurut (Dewa Ayu Mutiara Kirana Praba Dewi, 2023) HMAC-SHA256 memberikan tingkat keamanan yang baik dan efisien untuk mendukung pertukaran pesan secara instan dan aman. Token PASETO juga pada saat ini sudah ada versi protokol yang terbaru yaitu V4. Oleh karena itu, penelitian lanjutan terkait implementasi JWT menggunakan algoritma HMAC-SHA256 dan token PASETO V4 belum dilakukan.

Program pasar murah adalah upaya stabilisasi harga pangan yang diluncurkan pemerintah sejak 2017 dengan menunjuk Perum Bulog sebagai salah satu pelaksana. Program ini merupakan bentuk turunan

dari operasi pasar, namun memiliki perbedaan dalam mekanismenya. Pada pasar murah, bahan pangan pokok dijual langsung kepada masyarakat dengan harga di bawah pasar atau sesuai dengan harga eceran tertinggi (HET). Sementara itu, operasi pasar dilakukan dengan cara menambah pasokan beras di pasar (Proborini et al., 2018).

Tujuan utama dari pasar murah yaitu untuk mengurangi permintaan terhadap pasar sehingga diharapkan harga di pasar dapat turun karena berkurangnya permintaan dan kemudian dapat mengendalikan harga secara umum. Stabilisasi harga melalui pasar murah dapat terjadi apabila pasar murah melakukan intervensi tepat pada waktu (bulan) dimana harga beras akan naik, seperti pada saat menjelang hari raya besar keagamaan atau saat musim paceklik. Stabilisasi harga inilah yang menjadi output dari dilaksanakannya pasar murah dimana output tersebut dapat tercapai apabila pelaksanaan pasar murah berjalan efektif.

Rakyat yang menjadi sasaran pasar murah adalah mereka yang secara ekonomi kurang memiliki daya beli, sehingga dengan adanya program pasar murah ini, dapat menjadi solusi bagi rakyat dalam memenuhi kebutuhan sembakonya. Namun program yang positif dari pemerintah ini, seringkali dalam pendistribusiannya tidak terselenggara dengan baik. Hal itu dibuktikan dengan kurangnya informasi kegiatan pasar murah kepada masyarakat, sehingga kesempatan ini dimanfaatkan oleh oknum untuk mengambil keuntungan, diantaranya dengan membeli paket sembako lebih dari batas pembelian. Kemudian permasalahan lain adalah distribusi tiket paket sembako yang tidak terawasi, sehingga seringkali masyarakat

yang tidak berhak menerima program ini bisa menikmatinya dan program ini tidak tepat sasaran.

Kemudian yang paling fatal dalam ketika pelaksanaan pasar murah atau pembagian bantuan lain adalah penyelenggara kurang mempersiapkan distribusi tiket paket sembako, sehingga pembagian tiket dilakukan di tempat kegiatan dan pada hari pelaksanaan, sehingga seringkali terjadi penumpukan masyarakat, karena takut tidak kebagian tiket yang mengakibatkan kericuhan pada saat pembagian sampai mengakibatkan korban

Berdasarkan latar belakang diatas, penulis membuat penelitian ini dengan judul "Studi Komparasi Kinerja Dan Keamanan *JSON Web Token* (JWT) Dan *Platform Agnostic Security Tokens* (PASETO) Pada *Restful API* Aplikasi Pasar Murah".

B. Rumusan Masalah

Berdasarkan latar belakang serta permasalahan yang telah disampaikan di atas, maka fokus penelitian ini adalah :

1. Bagaimanan implementasi protokol JWT dan PASETO pada Aplikasi Pasar Murah ?
2. Bagaimana perbandingan kinerja dan keamanan antara JWT dengan PASETO ?
3. Bagaimana hasil analisis perbandingan kinerja dan keamanan antara JWT dengan PASETO ?

C. Batasan Masalah

Dengan mempertimbangkan berbagai perkembangan yang mungkin muncul dari permasalahan yang telah dirumuskan, maka diperlukan penetapan batasan masalah yang jelas agar penelitian ini memiliki fokus dan tidak bias. Batasan-batasan yang ditetapkan dalam penelitian ini adalah sebagai berikut:

1. Ruang lingkup penelitian kami, berfokus pada implementasi protokol JWT dan PASETO pada Aplikasi Pasar Murah.
2. Pengukuran kinerja dan keamanan dari protokol protokol JWT dan PASETO berdasarkan waktu pembuatan token, ukuran token, dan waktu transfer token serta Top 3 OWASP API Security 2023.

D. Tujuan Penelitian

Dengan melakukan perbandingan kinerja dan keamanan pada protokol JWT dan PASETO yang diterapkan pada Aplikasi Pasar Murah, dapat diperoleh tujuan dari penelitian ini, yakni:

1. Membuat model arsitektur *Restful* API dengan menerapkan protokol JWT dan PASETO pada sistem Aplikasi Pasar Murah.
2. Memberikan hasil analisis perbandingan kinerja dan keamanan protokol JWT dan PASETO

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan sejumlah manfaat, baik secara teoritis maupun praktis. Adapun manfaat penelitian ini diantaranya adalah :

1. Mengetahui kelebihan dan kekurangan dalam penerapan protokol JWT dan PASETO yang diterapkan pada sistem otentikasi *login* Aplikasi Pasar Murah.
2. Menunjukan hasil perbandingan pengujian kinerja dan keamanan protokol JWT dan PASETO.
3. Memberikan rekomendasi dari pengukuran perbandingan kinerja dan keamanan protokol JWT dan PASETO.

BAB V
PENUTUP

A. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dan uraian yang telah dibahas sebelumnya, dapat disimpulkan sebagaimana berikut:

1. Implementasi protokol JWT dan PASETO Berhasil diimplementasikan pada sistem Aplikasi Pasr Murah. Namun berdasarkan pengujian yang telah dilaksanakan, terdapat perbedaan baik dari parameter kinerja atau performa maupun keamanan antara JWT dan PASETO. Pada pengujian dengan parameter waktu rata-rata waktu pembuatan token JWT adalah 1.68 *ms* , sedangkan PASETO adalah 2.35 *ms.* Selain itu, terdapat perbedaan juga pada pengujian waktu transfer token, dimana kecepatan transfer token JWT adalah 31.62 *ms* , sedangkan PASETO adalah 35.94 *ms.* Ukuran token yang dihasilkan oleh JWT adalah 809 *byte* , sedangkan PASETO adalah 839 *byte* . Hal ini menunjukkan bahwa PASETO menghasilkan lebih banyak token daripada JWT. Secara keseluruhan, berdasarkan hasil pengujian kinerja, dapat disimpulkan bahwa JWT memiliki kinerja yang lebih baik daripada PASETO.
2. Berdasarkan hasil pengujian keamanan terhadap token JWT dan PASETO, dengan menggunakan parameter *Top 3 OWASP*

API Security 2023 menunjukkan bahwa token JWT terbukti aman, namun rentan terhadap *Broken User Authentication* yang berfokus pada eksploitasi algoritma header dan dekode *payload*. Selanjutnya untuk PASETO Berdasarkan hasil pengujian keamanan, token PASETO terbukti aman serta memiliki keunggulan keamanan dibandingkan JWT. PASETO terbukti aman terhadap kerentanan yang diuji, sementara JWT menunjukkan kerentanan dalam beberapa aspek, seperti eksploitasi algoritma header dan *decode* payload token.

B. SARAN

1. Seiring dengan perjalanan waktu, RESRful API akan terus berkembang dengan standar keamanan-keamanan yang baru. Selain node.js, sekarang ini ada jenis *runtimes* lain seperti Bun bisa diimplementasikan pada RESTful API. Kemudian dari sisi algoritma yang digunakan, baik itu untuk protokol JWT maupun PASETO juga bergam, sehingga bisa menjadi opsi penelitan selanjutnya.
2. Dalam hal otentifikasi bisa dikemabangkan bukan hanya dengan menggunakan username dan password tetapi bisa dikembangkan dengan otentifikasi lewat citra Gambar atau barcode. Hal ini bisa meminimalisis celah kerentanan keamaman yang disebabkan oleh penggunaan username dan password.

DAFTAR PUSTAKA

Anugrah, I. G., & Fakhruddin, M. A. R. I. (2020). Development Authentication and Authorization Systems of Multi Information Systems Based REst API and Auth Token. *Innovation Research Journal*, *1*(2), 127. https://doi.org/10.30587/innovation.v1i2.1927

Darmawan, I., Umar Mansyur, M., Zulfana Imam, K., Moh. Syahdan, & Fawaid, A. (2023). Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem Informasi Akademik. *Jurnal Informasi Dan Teknologi*, *5*(2), 120–128. https://doi.org/10.37034/jidt.v5i2.368

Dewa Ayu Mutiara Kirana Praba Dewi. (2023). *Analisis Penggunaan HMAC-SHA256 pada Keamanan Aplikasi Chatting*. *18220084*. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-

Fandopa, J. A., & Santoso, N. (2022). Pengembangan Sistem Informasi Manajemen Percetakan pada Gajayana Digital Printing Kota Malang berbasis Website. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *6*(11), 5371–5379. http://j-ptiik.ub.ac.id

Farchani, S. B., Hermanto, N., & Kusuma, B. A. (2025). Implementasi Rest Api Dalam Pengembangan Backend Inventory Peminjaman. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *10*(2), 1404–1413. https://doi.org/10.29100/jipi.v10i2.6249

Febrianto Widyoutomo, Hamidillah Ajie, & Widodo. (2021). Pengembangan Web Service Modul Mahasiswa Pada Sistem Informasi Akademik Universitas Negeri Jakarta. *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, *5*(1), 68–75. https://doi.org/10.21009/pinter.5.1.9

Fried Sinlae, Kalmany, L. K., Ruly Setiaji, & Syahrul, M. (2024). Menjelajahi Dunia Web: Panduan Pemula Untuk Pemrograman Web. *Jurnal Siber Multi Disiplin*, *2*(2), 107–118. https://doi.org/10.38035/jsmd.v2i2.170

Gunawan, R., & Rahmatulloh, A. (2019). *Gunawan Rahmatulloh, 2019*. *5*(1), 74–79.

Hartono, H. (2013). Pengertian Website dan Unsur-Unsurnya. *Ilmu Teknologi Informasi (Ilmuti)*.

Lunak, R. P., Medan, U. D., Yos, J. K. L., No, S., & Utara, S. (2020). *PENGEMBANGAN SISTEM OTENTIKASI PADA SEBUAH APLIKASI YANG BERBASISKAN WEB*. *1*(1), 1–9.

Mansur, E. S., Rahmatulloh, A., Shofa, R. N., & Darmawan, I. (2023). AMAN : Token-based Authentication to Improved Single Sign-On Security Between Systems. *2023 International Conference on Advancement in Data Science, E-Learning and Information System (ICADEIS)*, 1–6. https://doi.org/10.1109/ICADEIS58666.2023.10270904

Maulana Awangga, R., Ardhya Bisma, M., Rifqi, M., & Ulhaq, D. (2024). Whatsauth: Single Sign On Cerdas Berbasis 2FA dan WebSocket. *Jurnal Teknik Informatika*, *16*(2), 22–26. https://github.com/whatsauth/.

Mestre, P., Madureira, R., Melo-Pinto, P., & Serodio, C. (2018). Multiple JSON web tokens for mobile distributed applications. *Engineering Letters*, *26*(2), 281–286.

Nashikhuddin, A. Y., Karaman, J., & Litanianda, Y. (2023). Implementasi Api Restful Dengan Json Web Token (Jwt) Pada Aplikasi E-Commerce Thrifty Shop Untuk Otentikasi Dan Otorisasi Pengguna. *METHOMIKA Jurnal Manajemen Informatika Dan Komputerisasi Akuntansi*, *7*(2), 239–246. https://doi.org/10.46880/jmika.vol7no2.pp239-246

Nugraha, A. F., Kabetta, H., Buana, I. K. S., & Hadiprakoso, R. B. (2023). Performance and Security Comparison of Json Web Tokens (JWT) and Platform Agnostic Security Tokens (PASETO) on RESTful APIs. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, 15–22. https://doi.org/10.1109/ICoCICs58778.2023.10277377

Nurchasanah, I., & Palasara, N. D. (2025). Analisis Restful Api Web Service Pada Sistem Informasi Barbershop. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *12*(1), 276–293. https://doi.org/10.35957/jatisi.v12i1.10404

Nurlailah, E., & Nova Wardani, K. R. (2023). Perancangan Website Sebagai Media Informasi Dan Promosi Oleh-Oleh Khas Kota Pagaralam. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(4), 1175–1185. https://doi.org/10.29100/jipi.v8i4.4006

Painem, P., & Soetanto, H. (2020). Sistem Presensi Pegawai Berbasis Web Service Menggunakan Metode Restfull Dengan Keamanan JWT Dan Algoritma Haversine. *Fountain of Informatics Journal*, *5*(3), 6. https://doi.org/10.21111/fij.v5i3.4906

Parlika, R., N, R. S., Andreanto, B., R, M. I., & M, A. F. (2019). Implementasi Otentikasi Dengan Teknologi Qr-Code Berbasis Android Menggunakan Codeigniter Dan React Native. *E-NARODROID*, *5*(2), 56–67. https://doi.org/10.31090/narodroid.v5i2.934

Proborini, A., Ekowati, T., & Sumarjono, D. (2018). Analisis Efektivitas Pelaksanaan Pasar Murah Bulog Dalam Menjaga Stabilitas Harga Beras di DKI Jakarta Anita Proborini 1 , Titik Ekowati 1 , Djoko Sumarjono 1 1. *Jurnal Pendidikan Bisnis Dan Ekonomi*, *4*(1), 38–49.

Putra, A. W. P., Bhawiyuga, A., & Data, M. (2018). Implementasi Otentikasi JSON Web Token (JWT) Sebagai Mekanisme Otentikasi Protokol MQTT Pada Perangkat NodeMCU. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(2), 584–593.

Rahmatulloh, A., Sulastri, H., & Nugroho, R. (2018). Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (JNTETI)*, *7*(2). https://doi.org/10.22146/jnteti.v7i2.417

Riandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*, *4*(3), 160–165. https://doi.org/10.37034/jidt.v4i3.236

Series, I. O. P. C., & Science, M. (2019). *Performance comparison of signed algorithms on JSON Web Token Performance comparison of signed algorithms on JSON Web Token*. https://doi.org/10.1088/1757-899X/550/1/012023

Setiawan, A., & Purnamasari, A. I. (2020). Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk Otentikasi Aplikasi BatikKita. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 4–10. https://doi.org/10.29207/resti.v4i6.2533

Sitorus, N. F., Kusyanti, A., & Bhawiyuga, A. (2020). *Implementasi Otentikasi Berbasis Token Menggunakan Platform- Agnostic Security Tokens (PASETO) Sebagai Mekanisme Autentikansi RESTful API*. *4*(11).

Taofik, I., Aprilman, H., Fadillah, M., & Pardamean, J. (2023). *Implementasi JSON Web Token (JWT) untuk Authentication Data pada Aplikasi Bayeue Dengan Algoritma HMAC SHA- 256*. *1*(10), 4–10. https://doi.org/10.13140/RG.2.2.33916.55680

Darmawan, I, A. P. A. Karim, A. Rahmatulloh, R. Gunawan and D. Pramesti, "JSON Web Token Penetration Testing on Cookie Storage with CSRF Techniques," 2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS), Bali, Indonesia, 2021, pp. 1-5, doi: 10.1109/ICADEIS52521.2021.9701965.