

Optimasi Keamanan dalam Pengembangan Aplikasi Menggunakan Metode *Agile Scrum* dan *JSON Web Token*

¹Huda Prasetyo, ²Ucu Nugraha

^{1,2}Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Bandung, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

This research discusses ease and security in application development by utilizing the Agile Scrum and JSON Web Token (JWT) methods. The aim is to provide guidance to application developers so they can develop software solutions more efficiently and quickly and maintain a good level of security. The research was carried out systematically and clearly, with the hope that the application of the Agile Scrum and JWT methods can complete application development effectively and safely. Most developers still use traditional methods such as waterfall or session, which may have set goals and default configurations at the start of development but are less responsive to sudden changes or client requests. Therefore, implementing Agile Scrum and JWT methods is very important to overcome these challenges. The Agile Scrum method enables high adaptability and responsiveness to changes in application development, while JWT provides a strong layer of security. Collaboration between the two can help create applications that are easier, clearer, and have high added value. This way, developers can better prepare for development challenges and produce better application solutions. This means that the application of Agile Scrum and JWT in application development not only brings convenience to the process but also strengthens security aspects, creating a development environment that is adaptive and responsive to the dynamics of application needs.

Keywords: Security, Application Development, Agile Scrum Method, JSON Web Token

ABSTRAK

Penelitian ini membahas tentang kemudahan dan keamanan dalam pengembangan aplikasi dengan memanfaatkan metode Agile Scrum dan JSON Web Token (JWT). Tujuannya adalah memberikan panduan kepada para pengembang aplikasi agar mampu mengembangkan solusi perangkat lunak dengan lebih efisien, cepat, dan menjaga tingkat keamanan dengan baik. Penelitian dilakukan secara sistematis dan jelas, dengan harapan bahwa penerapan metode Agile Scrum dan JWT dapat menyelesaikan pengembangan aplikasi secara efektif dan aman. Sebagian besar pengembang masih menggunakan metode tradisional seperti Waterfall atau Session, yang mungkin telah menetapkan tujuan dan konfigurasi baku pada awal pengembangan, tetapi kurang responsif terhadap perubahan mendadak atau permintaan klien. Oleh karena itu, penerapan metode Agile Scrum dan JWT menjadi sangat penting untuk mengatasi tantangan tersebut. Metode Agile Scrum memungkinkan adaptabilitas dan responsivitas tinggi terhadap perubahan dalam pengembangan aplikasi, sementara JWT memberikan lapisan keamanan yang kuat. Kolaborasi keduanya dapat membantu menciptakan aplikasi yang lebih mudah, jelas, dan memiliki nilai tambah yang tinggi. Dengan demikian, para pengembang dapat menghadapi tantangan pengembangan dengan lebih siap dan menghasilkan solusi aplikasi yang lebih baik. Artinya, penerapan Agile Scrum dan JWT dalam pengembangan aplikasi tidak hanya membawa kemudahan dalam proses, tetapi juga memperkuat aspek keamanan, menciptakan lingkungan pengembangan yang adaptif dan responsif terhadap dinamika kebutuhan aplikasi.

Kata Kunci: Keamanan, Pengembangan Aplikasi, Metode Agile Scrum, JSON Web Token

1. PENDAHULUAN

Agile, Scrum, dan JSON Web Token (JWT) menjadi trinitas yang tak terpisahkan dalam metode pengembangan aplikasi. Secara keseluruhan, inti dari kombinasi Agile Scrum dan JWT adalah penyediaan metode dan alat yang mampu meningkatkan efisiensi dan manajemen pengembangan aplikasi, sehingga hasilnya lebih optimal dan terkelola dengan baik. Meskipun demikian, saat ini masih banyak perusahaan atau manajer proyek yang belum mengadopsi Agile Scrum dan JWT dalam praktik pengembangan aplikasinya. Dampaknya terlihat pada kualitas aplikasi yang tidak mencapai tingkat optimal dan tidak memenuhi target yang ditetapkan [1], [2].

Ketidakimplementasian Agile Scrum dan JWT ini tidak hanya memengaruhi tingkat efisiensi pengembangan aplikasi, tetapi juga menciptakan kerugian finansial yang signifikan, terutama bagi perusahaan yang fokus pada pengembangan aplikasi di era modern ini[3]. Perusahaan-perusahaan besar sering menghadapi berbagai masalah dalam pengembangan aplikasi, terutama yang tidak mengadopsi metode Agile Scrum dan JWT. Tantangan seperti proyek yang terlambat, kurang terorganisir, tidak efisien, dan tidak aman dapat merugikan bisnis[4]. Selain itu, kondisi ini dapat menyebabkan ketidaknyamanan bagi karyawan, merendahkan semangat kerja, dan merugikan pencapaian dalam proses pengembangan aplikasi[5]. Dengan demikian, implementasi Agile Scrum dan JWT bukan hanya sebagai pilihan, melainkan suatu kebutuhan yang strategis dalam memastikan keberhasilan pengembangan aplikasi[6].

Tujuan penelitian ini adalah untuk menyelidiki kemudahan dan keamanan dalam pengembangan aplikasi dengan memanfaatkan metode Agile Scrum dan JSON Web Token (JWT). Penelitian ini bertujuan memberikan panduan kepada para pengembang aplikasi agar dapat mengembangkan solusi perangkat lunak dengan tingkat efisiensi yang optimal, mempercepat proses pengembangan, dan menjaga tingkat keamanan dengan baik.

2. TINJAUAN PUSTAKA

Pengembangan Aplikasi Menggunakan Metode Agile Scrum

Dalam dunia struktur organisasi, beberapa tren menonjol, seperti *Agile Organization*, *Horizontal Organization*, dan *Network Organization*. Namun, yang paling menonjol di antara mereka adalah konsep Agile. *Agile Organization* dapat diartikan sebagai organisasi yang gesit, mampu bergerak cepat dalam pekerjaan dan mencapai tujuan perusahaan dengan efisien. *Agile Organization* membedakan diri dengan beberapa karakteristik khusus. Pertama, perusahaan yang menerapkan Agile cenderung mengandalkan peluang untuk mengelola informasi dengan lebih baik. Kedua, ketika menghadapi eksekusi suatu aksi, tanggung jawab biasanya dipegang oleh individu tertentu, seperti *Project Manager* [7]. Selanjutnya, organisasi yang menganut Agile cenderung bertindak dengan proaktif, mengantisipasi kendala atau masalah yang mungkin timbul. Keputusan di lingkungan Agile bisa diambil dengan cepat karena setiap orang bekerja bersama eksekutif yang dapat memberikan solusi saat dibutuhkan[8]. Selain itu, proses implementasi aksi menjadi lebih mudah karena beberapa elemen yang tidak esensial dalam bisnis dapat dihapuskan. Dengan menerapkan Agile, perusahaan dapat mengoptimalkan efisiensi, responsivitas, dan manajemen risiko, menciptakan lingkungan di mana keputusan diambil dengan cepat dan tindakan dapat diimplementasikan dengan lebih lancar[9].

Scrum, yang pertama kali diperkenalkan pada tahun 1986 oleh Hirotaka Takeuchi dan Ikujiro Nonaka dalam artikel berjudul "*The New Product Development Game*" di *The Harvard Business Review*, menggunakan metafora untuk membandingkan dua pendekatan berbeda. Menurut Takeuchi dan Nonaka, tim yang beroperasi seperti 'pelari estafet' dianggap ketinggalan jaman, sementara mereka meyakini bahwa model kerja yang lebih kolaboratif seperti 'tim rugby' akan memberikan kekuatan kepada perusahaan untuk bersaing dalam lingkungan bisnis global[10]. Pada tahun 1993, beberapa tahun setelah pengenalan Scrum oleh Takeuchi dan Nonaka, John Sutherland, John Scumniotales, dan Jeff McKenna mengumumkan bahwa mereka telah mengadopsi dan menguji penerapan Scrum di Easel Corp. Pengalaman praktis ini memberikan kontribusi pada pengembangan lebih lanjut dan pemahaman terhadap efektivitas metode Scrum dalam mengelola proyek dan meningkatkan produktivitas tim pengembangan. Scrum memiliki dasar-dasar yang mencakup prinsip-prinsip kunci untuk memastikan kelancaran dan kualitas dalam pengembangan perangkat lunak[11]. Pertama, transparansi adalah nilai utama yang menuntut agar semua pekerjaan dalam tim perusahaan dapat diketahui oleh setiap anggota. Ini mencakup informasi seperti estimasi waktu, bobot pekerjaan, kolaborasi, dan saling bantu-membantu di antara anggota tim. Kedua, prinsip *Inspection* mendorong tim untuk terus memantau hasil produk yang sedang dikembangkan. Umumnya, *Project Manager* bertanggung jawab untuk memeriksa hasil produk secara berkala. Terakhir, prinsip *Adaptation* mewajibkan seluruh tim untuk beradaptasi dengan dinamika pekerjaan dan perubahan waktu. Tujuannya adalah untuk menghasilkan produk dengan kualitas yang lebih kuat melalui penyesuaian

yang terus-menerus. Dengan demikian, dasar-dasar Scrum memberikan kerangka kerja yang kokoh untuk memastikan proyek pengembangan perangkat lunak berjalan efisien dan menghasilkan produk berkualitas tinggi[12].

Pada tahun 2001, terjadi tonggak sejarah dalam dunia pengembangan perangkat lunak dengan pembentukan *Agile Manifesto* oleh sejumlah ahli yang menciptakan metodologi di bidang *Software Development*. *Manifesto* ini memicu transisi para ahli dari metode tradisional, seperti *Waterfall*, yang pada masa itu umumnya digunakan dalam pengembangan perangkat lunak[13]. *Waterfall* adalah sebuah metodologi yang beroperasi secara berurutan atau linier dalam *Software Development*, dengan tahapan analisis, desain, implementasi, pengujian, penyebaran, dan pemeliharaan. Namun, metode ini dianggap kurang efektif atau tidak sesuai untuk diimplementasikan dalam *Software Development*, terutama karena kurangnya fleksibilitas menghadapi perubahan mendadak yang sering terjadi dalam pengembangan aplikasi[13]. *Agile Manifesto*, yang menunjukkan nilai dan prinsip-prinsip, memberikan arah baru dengan penekanan pada proses, pengembangan aplikasi secara luas, kolaborasi dengan klien terkait kontrak pengembangan aplikasi, serta tanggung jawab terhadap perubahan seiring dengan berjalannya proses atau rencana yang telah ditetapkan[11]. Prinsip-prinsip ini mencerminkan pendekatan yang lebih adaptif dan responsif dalam mengelola proyek pengembangan perangkat lunak.

Optimasi Keamanan dalam Pengembangan Aplikasi Menggunakan JSON Web Token

JSON Web Token (JWT) adalah sebuah protokol terbuka yang menggunakan format JSON (*Javascript Object Notation*) untuk mentransmisikan informasi secara aman antar pihak[14]. JWT sering digunakan sebagai mekanisme otentikasi untuk mengamankan transfer data antara pengguna dan server. Token JWT memiliki format yang terdiri dari tiga bagian, yaitu *header*, *payload*, dan *signature*, yang dihasilkan dalam format JSON[15]. Sebagai contoh, sebuah token JWT mungkin terlihat seperti ini: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. Jika diuraikan, *output*-nya akan menjadi sebuah struktur JSON seperti `{“name”: “john doe”}`, yang menjelaskan data tertentu dalam token dengan format yang mudah dibaca[15].

JSON Web Token (JWT) beroperasi dengan prinsip mirip kata sandi, namun dengan metode enkripsi yang menghasilkan serangkaian karakter acak. Saat diartikan, karakter tersebut mengungkapkan data dalam format JSON. Salah satu keunggulan JWT adalah kemampuannya untuk mengatur masa aktif, sehingga token akan kedaluwarsa setelah waktu tertentu. Ini memberikan lapisan keamanan tambahan, memastikan bahwa data sensitif hanya dapat diakses dalam jangka waktu yang ditentukan. Selain itu, keunggulan lainnya dari JWT adalah kemampuannya sebagai alat pengembangan *multi-platform*, memungkinkan penggunaannya secara universal di berbagai *platform* seperti *Mobile*, *Web*, *Desktop*, dan lainnya[16].

JSON Web Token (JWT) menggunakan *signature* sebagai mekanisme untuk memastikan integritas dan otentikasi data. *Signature* ini ditempatkan di bagian terakhir JWT dan dihasilkan dengan menerapkan algoritma kriptografi tertentu, seperti HMAC atau RSA. Proses pembuatan *signature* melibatkan *header* dan *payload* JWT, yang digabungkan dengan *secret key* yang hanya diketahui oleh pihak yang berwenang. Tujuan utamanya adalah membuktikan bahwa JWT tidak mengalami perubahan sejak dibuat. Ketika JWT diterima oleh pihak yang dituju, mereka menggunakan *secret key* yang sama dan algoritma yang identik untuk memverifikasi *signature*. Keberhasilan verifikasi menandakan bahwa JWT *valid* dan dapat diandalkan dalam hal integritas datanya. Menjaga kerahasiaan *secret key* adalah kunci dalam penggunaan JWT. Jika *secret key* jatuh ke tangan yang salah, maka JWT dapat dimanipulasi, dan *signature* palsu dapat dihasilkan. Oleh karena itu, penting untuk memprioritaskan keamanan dan kerahasiaan *secret key* agar dapat memastikan keandalan dan keabsahan JWT[17].

JWT menonjol sebagai pilihan yang tepat untuk mengamankan sistem dengan beberapa alasan kunci. Pertama, autentikasi menjadi lebih aman karena adanya verifikasi data melalui token yang dikirim. Dengan menggunakan algoritma kriptografi yang aman, hanya pihak-pihak yang dipercayai oleh sistem yang dapat menggunakan token ini, meningkatkan tingkat keamanan autentikasi. Kedua, kelebihan JWT terletak pada sifatnya yang dinamis, yang berdiri sendiri tanpa memerlukan *server*

atau konfigurasi lanjutan untuk integrasi dengan sistem lainnya. Hanya *secret key* yang dibutuhkan, yang hanya dapat diakses oleh pihak-pihak yang dipercayai, menjadikannya solusi yang mudah diimplementasikan. Ketiga, keamanan tambahan hadir melalui fitur kadaluarsa dalam token JWT. Karena token ini berdiri sendiri, JWT memungkinkan pengaturan waktu kadaluarsa yang dapat mengatur waktu berlakunya token. Jika token sudah kadaluarsa, data tidak dapat diolah dan diproses oleh sistem, meningkatkan keamanan data. Keempat, JWT memberikan kemudahan dalam sistem revoke atau pencabutan token yang masih aktif. Ini menjadi keuntungan dalam aspek keamanan, di mana jika token berada di tangan yang salah, sistem dapat mencabut otorisasi dari token tersebut, menjadikannya tidak dapat digunakan kembali dan dimasukkan ke dalam daftar hitam. Terakhir, dalam pertukaran data yang aman, JWT menggunakan enkripsi yang andal. Ini memastikan bahwa ketika terjadi pertukaran data, terutama informasi sensitif yang dikirim melalui JWT, data tersebut tersimpan dengan aman dan hanya dapat diakses oleh pihak-pihak yang berwenang. Dengan demikian, JWT memberikan keamanan dan kontrol yang diperlukan dalam pengelolaan autentikasi dan pertukaran data [18].

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian deskriptif, suatu pendekatan yang digunakan untuk menjelaskan kejadian sesuai dengan fakta yang teramati. Tujuan utama metode ini adalah memberikan gambaran yang jelas mengenai apa yang terjadi dan apa yang telah diobservasi. Dalam konteks penelitian ini, data dijabarkan untuk menciptakan perbandingan yang obyektif dengan berbagai artikel yang telah ada, menjadikannya acuan yang kuat untuk mendukung hasil penelitian. Metode penelitian deskriptif memungkinkan peneliti untuk merinci informasi yang telah dikumpulkan dengan cermat, membantu memahami dan menjelaskan fenomena yang diteliti. Dalam penelitian ini, fokusnya pada pembahasan dan perbandingan artikel-artikel yang relevan untuk mengevaluasi dan mendapatkan pemahaman yang lebih mendalam terkait isu tertentu. Dengan menggunakan pendekatan ini, diharapkan penelitian dapat menghasilkan data yang akurat dan menyeluruh untuk mendukung temuan yang obyektif. Melalui metode deskriptif, penelitian ini mencapai kejelasan dalam menjelaskan fenomena dan menganalisis data dengan teliti. Penggunaan metode ini memberikan landasan yang kokoh untuk memberikan gambaran menyeluruh tentang topik penelitian, memastikan bahwa hasil penelitian mencerminkan realitas dengan sebaik mungkin [19].

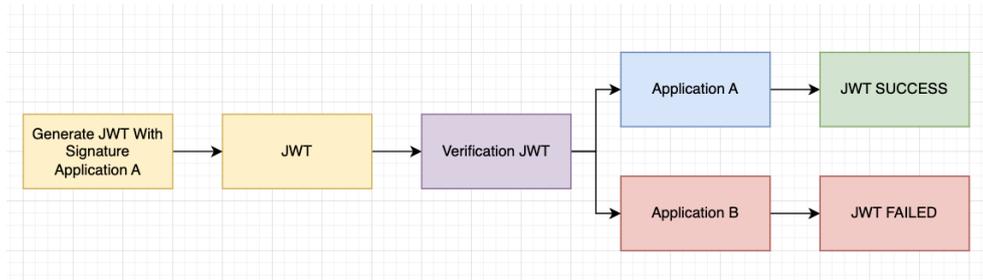
4. HASIL DAN PEMBAHASAN

Penelitian ini memanfaatkan bahasa pemrograman JavaScript dan NodeJS sebagai kerangka kerja untuk mengimplementasikan keamanan data dengan menggunakan JSON Web Token (JWT). Implementasi JWT pada *JavaScript* dapat dianggap relatif mudah karena memerlukan instalasi NodeJS, yang dapat dengan cepat diunduh dan dijalankan. Aplikasi yang digunakan dalam implementasi JWT ini mencakup beberapa komponen kunci, yaitu NodeJS yang diunduh melalui situs resmi <https://nodejs.org/en/download>, paket JWT yang diakses melalui <https://www.npmjs.com/package/jsonwebtoken>, Postman untuk pengecekan HTTP request, dan VsCode atau Notepad sebagai editor teks.

Sebelum memulai implementasi JWT, perlu dipahami gambaran arsitektur tentang bagaimana JWT bekerja dalam implementasi. Hal ini memberikan pemahaman dasar tentang proses yang terlibat dan membantu memetakan langkah-langkah implementasi dengan lebih baik. Gambaran arsitektur ini menjadi dasar bagi peneliti untuk merancang dan melaksanakan implementasi dengan tepat.

Proses implementasi JWT pada penelitian ini melibatkan langkah-langkah yang sistematis dan terstruktur. Tahap awal melibatkan instalasi NodeJS, yang merupakan langkah kunci untuk memulai pengembangan dengan *JavaScript*. Selanjutnya, pemasangan paket JWT adalah langkah penting untuk menambahkan fungsi keamanan menggunakan token pada aplikasi. Penggunaan Postman memberikan fasilitas untuk melakukan pengecekan HTTP *request*, memastikan bahwa mekanisme keamanan yang diimplementasikan berjalan dengan benar.

Seluruh rangkaian aplikasi dan langkah-langkah tersebut dirinci dan dijelaskan secara rinci dalam penelitian ini. Hal ini memastikan bahwa pembaca dapat mengikuti implementasi dengan mudah dan mendapatkan pemahaman yang mendalam tentang bagaimana keamanan data menggunakan JWT diterapkan dalam lingkungan *JavaScript* dan *NodeJS*.



Gambar 1. Cara Bekerja Sederhana dari JWT

Dapat dijelaskan dari Gambar 1 di atas bahwa JSON Web Token (JWT) memiliki karakteristik keunikan di mana token yang dibuat untuk suatu aplikasi akan *valid* hanya untuk aplikasi tersebut. Dengan kata lain, JWT yang dihasilkan untuk aplikasi A tidak akan memiliki validitas untuk aplikasi B. Jika upaya verifikasi dilakukan pada aplikasi B menggunakan JWT yang dibuat untuk aplikasi A, sistem akan mengembalikan pesan error yang menyatakan "*JWT Signature Invalid.*"

Karakteristik ini memastikan bahwa setiap aplikasi memiliki token yang bersifat eksklusif, meningkatkan tingkat keamanan dan menghindari risiko penyalahgunaan token antaraplikasi. Prinsip ini penting untuk menjaga integritas data dan memastikan bahwa hanya aplikasi yang memiliki hak akses yang sah yang dapat memverifikasi dan menggunakan token yang sesuai dengan identitas dan otorisasi pengguna.

Implementasi *JSON Web Token (JWT)*

Langkah-langkah implementasi JWT secara singkat di atas dapat diikuti untuk membangun aplikasi yang menggunakan JSON Web Token (JWT) dengan *NodeJS* dan *Express*. Berikut adalah penjelasan lebih rinci mengenai kode dan langkah-langkah tersebut:

- 1) Buka *Visual Studio Code (Vscode)* dan buat folder proyek baru. Di dalam folder tersebut, buka terminal dan inisialisasi proyek *NodeJS* dengan perintah:

```
bash Copy code
npm init -y
```

Gambar 2. Inisialisasi Proyek

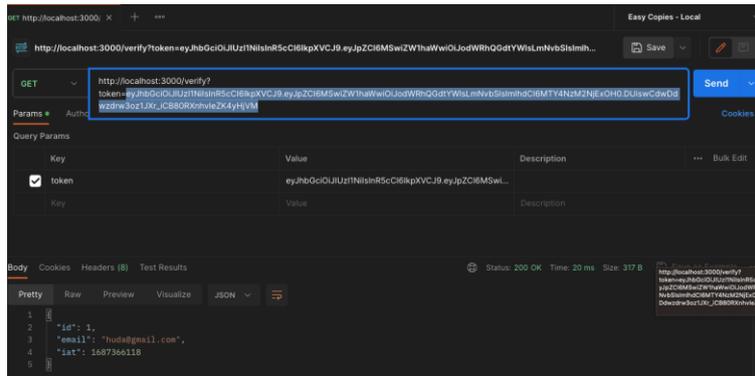
Selanjutnya, *install* beberapa *package* yang diperlukan, yaitu *Express*, *jsonwebtoken*, dan *cors*, dengan perintah:

```
bash Copy code
npm install express jsonwebtoken cors
```

Gambar 3. Install Package

- 2) Setelah inisialisasi proyek, buat file baru bernama *index.js* di dalam folder proyek. Isi file tersebut dengan kode berikut:

Jika token berhasil dibuat dan valid, Anda akan melihat respons balikan yang berisi token seperti {token: 'asdasdsd'}. Apabila tidak valid, respons akan memberikan informasi terkait ketidakvalidan token.



Gambar 7. Verifikasi Token JWT

Kemudian klik "Send". Data yang muncul berasal dari token dan akan ditampilkan dalam format JSON, contohnya {id: 1, email: 'huda@gmail.com', iat: 123123}. Gambar 3 di atas menunjukkan bahwa token yang dibuat valid dan dapat digunakan di dalam aplikasi tersebut.

5. KESIMPULAN

Kesimpulan dari penelitian Optimasi Keamanan dalam Pengembangan Aplikasi Menggunakan Metode Agile Scrum dan JSON Web Token (JWT) dapat dirangkum bahwa Agile dan Scrum terbukti memiliki keterkaitan yang erat dalam pengembangan aplikasi modern. Kombinasi keduanya membawa manfaat signifikan untuk memastikan proyek berjalan sesuai rencana dan lebih terfokus. Penggunaan Agile Scrum memberikan kemudahan dalam pengembangan aplikasi. Proses ini membuat manajemen proyek lebih transparan dan memungkinkan tim untuk lebih memikirkan keamanan dari berbagai perspektif. Penerapan JWT pada aplikasi membawa dinamisme, terutama dalam aspek keamanan. JWT memberikan lapisan keamanan yang efektif dan mudah diintegrasikan. Agile Scrum tidak hanya membuat pengembangan efisien, tetapi juga memberikan manajemen proyek yang lebih jelas. Kejelasan peran dalam tim membuat koordinasi antar anggota tim menjadi lebih mudah. Kombinasi Agile Scrum dan JWT memberikan efisiensi dan memastikan ketepatan waktu dalam pengembangan aplikasi. *Sprint Review* dan *Sprint Retrospective* membantu evaluasi dan pengembangan yang lebih baik. Tujuan suatu proyek menjadi pencapaian untuk memajukan perusahaan, dan keamanan yang diterapkan menggunakan JWT memberikan tingkat keamanan yang mumpuni. Agile Scrum memungkinkan tim untuk merespons perubahan permintaan klien tanpa memberatkan tim. Keputusan untuk menggunakan JWT dari awal memberikan landasan yang kuat untuk keamanan. Melalui *Sprint Retrospective*, Agile Scrum membantu evaluasi pekerjaan sebelumnya dan memberikan panduan untuk pengembangan yang lebih baik di masa depan. Penggunaan JWT memudahkan sistem untuk berkomunikasi dan berintegrasi dengan aplikasi lain. Hal ini krusial untuk mengakomodasi permintaan dan kebutuhan perusahaan yang berkembang. Agile Scrum dan JWT membantu menata dan mengatur manajemen perusahaan, khususnya pada aspek teknis, sehingga menciptakan suatu standar dalam pengembangan aplikasi. Dengan demikian, implementasi keseimbangan antara Agile Scrum dan JWT dapat menjadi kunci sukses dalam pengembangan aplikasi yang efisien, aman, dan adaptif terhadap perubahan.

6. DAFTAR PUSTAKA

- [1] I. Darmawan, M. U. Mansyur, K. Z. Imam, and M. Syahdan, "Evaluasi Keamanan Privilege Terintegrasi JSON Web Token pada Sistem Informasi Akademik," *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 120–128, 2023, doi: 10.37034/jidt.v5i1.368.
- [2] Z. I. Sholihati and I. Tahyudin, "Pengembangan Aplikasi Tiga-Tingkat Menggunakan Metode

- Scrum pada Aplikasi Presensi Karyawan Glints Academy,” *J. RESTI Rekayasa Sist. dan Teknol. Inf.*, vol. 6, no. 1, pp. 169–176, 2022.
- [3] M. F. Afrizzi, R. B. Hadiprakoso, and A. R. Kardian, “Rancang Bangun Aplikasi COOL : REST API Untuk Learning Management System,” *J. Ilm. Info Kripto*, vol. 17, no. 2, 2020.
- [4] F. X. Senduk, X. B. N. Najooan, and S. R. U. A. Sompie, “Development of Microservices Architecture with RESTful API Gateway using Backend-for- frontend Pattern in Higher Education Academic Portal,” *J. Tek. Inform.*, vol. 18, no. 1, pp. 315–324, 2023.
- [5] A. F. Ramadhan and A. Kurniawan, “Pengembangan Aplikasi Pencatatan dan Penganggaran Keuangan Pribadi Berbasis Webiste Dengan Metode Penganggaran Cash Only Budgeting,” *J. Manaj. Inform.*, vol. 15, no. 2, pp. 1–12, 2023.
- [6] Nasrul and A. Izhar, “PENGEMBANGAN REST API DENGAN MENGGUNAKAN EXPRESS JS UNTUK Mencari Mentor Pribadi,” *J. Inform. Terpadu*, vol. 9, no. 2, pp. 92–102, 2023.
- [7] P. B. Lowry and D. Wilson, “Creating agile organizations through IT: The influence of internal IT service perceptions on IT service quality and IT agility,” *J. Strateg. Inf. Syst.*, vol. 25, no. 3, pp. 211–226, 2016, doi: <https://doi.org/10.1016/j.jsis.2016.05.002>.
- [8] R. Mayefis *et al.*, *Rekayasa Perangkat Lunak*. Global Eksekutif Teknologi, 2023. [Online]. Available: <https://books.google.co.id/books?id=6wmpEAAAQBAJ>
- [9] E. Supriyadi, *Sistem Informasi Bisnis Dunia Versi 4.0*. Penerbit Andi, 2020. [Online]. Available: <https://books.google.co.id/books?id=krgrEAAAQBAJ>
- [10] H. Takeuchi and I. Nonaka, “The New Product Development Game,” *Harvard Bus. Sch.*, pp. 137–147, 1986.
- [11] Y. E. Rachmad *et al.*, *Rekayasa Perangkat Lunak*. PT. Sonpedia Publishing Indonesia, 2023. [Online]. Available: <https://books.google.co.id/books?id=JSeuEAAAQBAJ>
- [12] D. Hamidin, W. Rediana, and R. Andarsyah, “PENINGKATAN KUALITAS SEKOLAH DENGAN PELATIHAN TIK DAN BAHASA DAN MINAT BACA SISWA DI SD JUARA BANDUNG DAN CIMAHI,” *COMPETITIVE*, vol. 10, no. 1, p. 1, 2015.
- [13] S. Kiv, S. Heng, M. Kolp, and Y. Wautelet, “Agile Manifesto and Practices Selection for Tailoring Software Development: A Systematic Literature Review BT - Product-Focused Software Process Improvement,” 2018, pp. 12–30.
- [14] L. Bassett, *Introduction to JavaScript Object Notation: A To-the-Point Guide to JSON*. O’Reilly Media, 2015. [Online]. Available: <https://books.google.co.id/books?id=Qv9PCgAAQBAJ>
- [15] A. Rahmatulloh, H. Sulastri, and R. Nugroho, “Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512,” *JNTETI*, vol. 7, no. 2, 2018.
- [16] A. Hibsya and A. Wibowo, “Implementasi Fitur Keamanan dengan JSON Web Token dan Fitur Geo- tagging pada Aplikasi Web Service Training From Home,” *J. RESTI Rekayasa Sist. dan Teknol. Inf.*, vol. 4, no. 4, pp. 618–626, 2021.
- [17] M. R. Royani and A. Wibowo, “Implementasi Web Service pada Perusahaan Logistik menggunakan JSON Web Token dan Algoritma Kriptografi RC4,” *J. RESTI Rekayasa Sist. dan Teknol. Inf.*, vol. 4, no. 3, pp. 591–600, 2021.
- [18] Y. Putra, Y. Yunus, and Sumijan, “Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting,” *J. Sistim Inf. dan Teknol.*, vol. 3, no. 2, pp. 56–63, 2021, doi: 10.37034/jsisfotek.v3i2.44.
- [19] G. Ambrose and P. Harris, *Basics Design 08: Design Thinking*. AVA Publishing, 2010. [Online]. Available: <https://books.google.co.id/books?id=9klpFfZDnWgC>