Whatsauth: *Single Sign On* Cerdas Berbasis 2FA dan WebSocket

Rolly Maulana Awangga[1], Muhammad Ardhya Bisma[2], Muhammad Rifqi Daffa Ulhaq[3]

Sekolah Vokasi, Universitas Logistik dan Bisnis Internasional[123]

email: [1)] awangga@ulbi.ac.id [2)] bisma@ulbi.ac.id [3)] 1204045@std.ulbi.ac.id

Abstrak

Pembobolan sistem merupakan ancaman serius bagi keamanan informasi, terutama ketika ada celah seperti formulir *login* tanpa verifikasi *Captcha* dan penggunaan kata sandi yang mudah ditebak, yang memudahkan pihak yang tidak bertanggung jawab untuk masuk. Banyak kasus mencatat bahwa administrator sistem menggunakan kata sandi bawaan yang sama dan umum, menciptakan risiko tinggi terhadap manipulasi data yang tidak sah dalam sistem. Solusi otorisasi yang umum saat ini memanfaatkan server tambahan seperti LDAP dan *OAuth*, meskipun efektif, belum ramah lingkungan.

Penelitian ini bertujuan untuk menyediakan solusi autorisasi dan autentikasi yang tidak hanya efektif dalam mengatasi risiko pembobolan sistem, tetapi juga ramah lingkungan dengan emisi karbon yang rendah. Oleh karena itu, penelitian ini berfokus pada pengembangan sistem keamanan yang tidak hanya ramah pengguna, tetapi juga mengurangi dampak lingkungan dengan meminimalkan ketergantungan pada server eksternal. Hasil dari penelitian ini diharapkan dapat memberi kontribusi positif pada keamanan informasi dengan mempertimbangkan aspek keberlanjutan lingkungan.

Kata Kunci: *Authorization, Authentication, Websocket, 2FA.*

Abstract

System breaches are a serious threat to information security, especially when there are loopholes such as login forms without Captcha verification and the use of easy-to-guess passwords, which make it easy for irresponsible parties to log in. Many cases note that system administrators use the same and common default passwords, creating a high risk of unauthorized manipulation of data in the system. Current common authorization solutions utilizing additional servers such as LDAP and OAuth, although effective, have not been environmentally friendly.

This research aims to provide an authorization and authentication solution that is not only effective in overcoming the risk of system breaches, but also environmentally friendly with low carbon emissions. Therefore, this research focuses on developing a security system that is not only user-friendly, but also reduces environmental impact by minimizing dependence on external servers. The results of this research are expected to make a positive contribution to information security by considering environmental sustainability aspects.

Keywords: *Authorization, Authentication, Websocket, 2FA.*

1. PENDAHULUAN

Di era digital yang terus berkembang, keamanan informasi menjadi hal krusial yang memerlukan perhatian sungguh-sungguh. Keberadaan sistem autentikasi yang andal dan efektif jadi prioritas utama bagi banyak platform dan aplikasi, dengan 2-*Factor Authentication* (2FA) menjadi salah satu metode umum yang digunakan untuk meningkatkan keamanan *login*[1], [2]. Autentikasi dua faktor (2FA) adalah mekanisme penting untuk melindungi akun pengguna akhir dari serangan phishing dan penggunaan ulang kata sandi [3].

Walaupun begitu, tantangan muncul dalam menerapkan 2FA secara efisien dan praktis tanpa mengurangi kenyamanan pengguna[4].

Selain itu, kepedulian global terhadap emisi karbon dan dampaknya pada perubahan iklim menuntut pertimbangan khusus dalam mengembangkan perangkat lunak dan sistem komputer[5]. Penurunan emisi karbon di sektor teknologi informasi dan komunikasi jadi fokus utama untuk menciptakan dunia digital yang lebih hijau dan berkelanjutan[6].

Untuk menjawab tantangan tersebut, riset ini memperkenalkan *Whatsauth*, sistem autentikasi cerdas yang memadukan 2FA dan *WebSocket*. Desain *Whatsauth* memperhitungkan aspek rendah emisi karbon, memberikan mekanisme autentikasi yang efektif dan praktis, agar pengguna bisa mengakses beragam *platform* dan aplikasi dengan tingkat keamanan yang lebih baik. Teknologi *WebSocket* juga dimanfaatkan untuk meningkatkan responsivitas sistem autentikasi lewat komunikasi *real-time* antara *server* dan klien[7].

Di samping fokus pada keamanan dan responsivitas, riset ini menempatkan penekanan khusus pada pengembangan "*low emission carbon code*" dalam membangun *Whatsauth*. Pendekatan ini bermakna riset akan memanfaatkan metodologi pengembangan perangkat lunak yang *sustainable*, dengan menghitung dampak lingkungan dari kode yang dihasilkan. Tujuan utama riset ini adalah memberikan kontribusi positif dalam meningkatkan keamanan sistem autentikasi, menekan emisi karbon dalam pengembangan perangkat lunak, juga mempromosikan kepedulian dan tanggung jawab atas keberlanjutan lingkungan di sektor teknologi informasi dan komunikasi.

2. LANDASAN TEORI

2.1 WebSocket

Dalam konteks *WhatsAuth*, *WebSocket* digunakan untuk memfasilitasi komunikasi *real-time* antara pengguna dan server autentikasi[8]. Koneksi *WebSocket* memungkinkan pertukaran pesan yang cepat dan efisien, yang sangat penting untuk proses autentikasi dan otorisasi yang responsive[9]. Penggunaan *WebSocket* mengeliminasi kebutuhan untuk polling berulang yang biasanya diperlukan dalam aplikasi berbasis HTTP, sehingga meningkatkan efisiensi operasional dan pengalaman pengguna[10].

2.2 PASETO (*Platform-Agnostic Security Tokens*)

PASETO (*Platform-Agnostic SEcurity TOkens*) adalah alternatif untuk JWT (JSON *Web Tokens*) yang dirancang untuk meningkatkan keamanan dalam pertukaran token. PASETO menyediakan semua manfaat dari JWT tetapi dengan implementasi yang lebih ketat dan eksplisit, mengurangi kesalahan umum dalam implementasi JWT seperti kesalahan dalam konfigurasi algoritma penandatanganan[11]. PASETO menentukan versi dan tujuan token secara eksplisit, sehingga memperjelas penggunaan token tersebut dan memperkecil kemungkinan penyalahgunaan token.

2.3 HTTP dan *WebSocket*

HTTP adalah protokol yang tidak mempertahankan keadaan (*stateless*), di mana setiap permintaan dibuat secara terpisah dan tidak ada informasi yang disimpan antar permintaan[12]. Ini memungkinkan independensi dan skalabilitas yang tinggi tetapi mengurangi efisiensi pada aplikasi *real-time* yang membutuhkan pertukaran data cepat dan terus-menerus. Di sisi lain, *WebSocket*, meskipun secara teknis adalah *stateless* karena tidak menyimpan keadaan antar pesan, memungkinkan sesi komunikasi yang persisten melalui koneksi yang tetap terbuka, mengurangi latensi dan overhead yang terkait dengan pembuatan koneksi baru untuk setiap pertukaran data[13].

3. METODE PENELITIAN

Tahapan-Tahapan Diagram Alur Metodologi Penelitian. Dari metodologi penelitian yang diusulkan pada memiliki tahapan - tahapan yang dijabarkan, yaitu:

- Pembuatan Protokol: Pada tahap ini dilakukan pembuatan

protokol untuk autentikasi dan autorisasi dengan mengadaptasi dari protokol 2FA yang sudah ada. Protokol dirancang berdasarkan mekanisme otorisasi *WhatsApp* menggunakan QR *Code*.

- Pengembangan *Server* Authentikasi: Server autentikasi dikembangkan dengan antarmuka berbasis *web socket* yang lebih hemat sumber daya dibandingkan protokol LDAP atau *OAuth* yang menggunakan HTTP.
- Pengembangan Antar Muka: Antarmuka dikembangkan dengan konsep *micro frontend* ES6+ *vanilla* JS dan menggunakan CDN agar lebih efisien dalam hal biaya komputasi dan *delivery* konten.
- Integrasi 2FA: Integrasi 2FA dilakukan dengan memanfaatkan *WhatsApp* sebagai media autentikasi tambahan setelah proses *login* awal dengan *username* dan *password*.
- Implementasi *WhatsAuth*: *WhatsAuth* diimplementasikan pada sistem yang ada di ULBI, salah satunya Aptimas. Hal ini bertujuan untuk mengintegrasikan sistem otentikasi cerdas whatsauth pada aplikasi yang sudah ada.
- Perhitungan Komputasi: Komputasi server *WhatsAuth* diukur dengan Grafana untuk menganalisis konsumsi RAM, CPU, dan sumber daya lain yang digunakan.

4. HASIL DAN PEMBAHASAN

Dalam rangka memudahkan akses dan transparansi, repositori kode sumber aplikasi *WhatsAuth* dapat dilihat secara publik di situs *GitHub*, melalui tautan berikut: https://github.com/whatsauth/. Lebih lanjut, dokumentasi terperinci yang mendukung penggunaan dan pengembangan *WhatsAuth* tersedia secara *online* di https://whatsauth.github.io/.

Aplikasi *WhatsAuth* terdiri dari dua komponen utama, *frontend* dan *backend*. Pada bagian *frontend*, aplikasi ini mengimplementasikan konsep mikro *frontend* dengan menggunakan ES6+ untuk peningkatan modularitas dan skalabilitas. Kode sumber untuk komponen *frontend* dapat diakses di https://github.com/whatsauth/js. Di sisi lain, implementasi *backend* dibangun menggunakan bahasa pemrograman Go, yang dikenal dengan efisiensinya yang tinggi dan jejak karbon yang rendah, mendukung upaya keberlanjutan lingkungan. Kode sumber untuk *backend* tersedia di https://github.com/whatsauth/whatsauth.

5. KESIMPULAN DAN SARAN

Seiring penutupan penelitian ini, terdapat inovasi yang diwujudkan melalui pengembangan sistem autentikasi cerdas *WHATSAUTH* memberikan kontribusi signifikan baik dalam aspek teknologi maupun keberlanjutan lingkungan. Keberhasilan integrasi 2-*Factor Authentication* (2FA) dan *WebSocket* bukan hanya menempatkan *WHATSAUTH* sebagai pionir dalam responsivitas dan keamanan sistem, tetapi juga sebagai pelopor dalam praktek pengembangan teknologi yang bertanggung jawab secara ekologis. Kesadaran ini tidak hanya meningkatkan efisiensi operasional tetapi juga mendukung visi pengurangan dampak negatif terhadap lingkungan melalui praktik "*low emission carbon code*". Berdasarkan wawasan ini, berbagai saran strategis dan praktis telah disusun untuk mengarahkan penelitian masa depan dan mengoptimalkan penerapan teknologi yang tidak hanya inovatif tetapi juga ramah lingkungan.

5.1 Kesimpulan

Berdasarkan hasil dari penelitian ini, kesimpulan yang dapat diperoleh sebagai berikut :

1. Penelitian ini berhasil dalam mengembangkan sistem autentikasi cerdas *WHATSAUTH* yang menggabungkan 2-*Factor Authentication* (2FA) dan *WebSocket*, serta mempertimbangkan aspek keberlanjutan lingkungan dalam pengembangan perangkat lunak.
2. Penelitian ini menunjukkan bahwa *WHATSAUTH* dapat meningkatkan keamanan *login*, responsivitas sistem, dan kesadaran terhadap keberlanjutan lingkungan di bidang teknologi informasi dan komunikasi.

3. Penelitian ini menyoroti pentingnya menerapkan praktik "*low emission carbon code*" dalam pengembangan perangkat lunak untuk mengoptimalkan penggunaan sumber daya, mengurangi pemakaian energi, dan meminimalkan emisi karbon.

5.2 Saran

Saran yang dapat diperoleh dari penelitian ini sebagai berikut:

1. Untuk penelitian masa depan, penelitian dapat dilanjutkan untuk mengembangkan sistem autentikasi yang lebih efisien dan ramah lingkungan
2. Penelitian tentang penerapan praktik "low emission carbon code" dalam pengembangan perangkat lunak juga dapat diperluas secara lebih lanjut, mengfokus pada cara mengurangi dampak lingkungan dalam proses pengembangan dan penggunaan perangkat lunak.
3. Penelitian ini juga dapat diperluas secara lebih lanjut untuk mengkaji dampak kebijakan dan praktik yang diadopsi dalam pengembangan sistem autentikasi terhadap keberlanjutan lingkungan.

6. DAFTAR PUSTAKA

[1] A. Ometov, S. V Bezzateev, N. Mäkitalo, S. D. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptogr.*, vol. 2, p. 1, 2018, [Online]. Available: https://api.semanticscholar.org/CorpusID:13698134

[2] O. O. Anyiam, U. A. Okengwu, and F. N. Anyiam, "An Enhanced Result Processing and Checking System for Public Universities using 2FA and TOTP," *International Journal of Engineering Research and*, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:219133665

[3] M. Golla, G. Ho, M. L\~ohmus, M. Pulluri, and E. M. Redmiles, "Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns," in *USENIX Security Symposium*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:236317681

[4] J. Reynolds *et al.*, "Empirical Measurement of Systemic 2FA Usability," in *USENIX Security Symposium*, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:221178505

[5] M. A. Raza *et al.*, "Modelling and development of sustainable energy systems," *AIMS Energy*, 2023, [Online]. Available: https://api.semanticscholar.org/CorpusID:257551959

[6] A. K. R. Jha, A. S. G. Andrae, and B. Mainali, "Comparison of Methods for Calculating Indirect Upstream Carbon Emissions from Information and Communication Technology Manufacturing," *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT*, 2023, [Online]. Available: https://api.semanticscholar.org/CorpusID:264071075

[7] A. O. Bavenko and A. Koba, "Using WebSocket technology for realtime data transfer," 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:226672572

[8] N. Sharma and R. Agarwal, "HTTP, WebSocket, and SignalR: A Comparison of Real-Time Online Communication Protocols," *Lecture Notes in Computer Science*, pp. 128–135, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-44084-7_13.

[9] A. S. Abdelfattah, T. Abdelkader, and E.-S. M. EI-Horbaty, "RAMWS: Reliable approach using middleware and WebSockets in mobile cloud computing," *Ain Shams Engineering Journal*, vol. 11, no. 4, pp. 1083–1092, Dec. 2020, doi:

https://doi.org/10.1016/j.asej.2020.04.002.

[10] M. I. Tarrés-Puertas, Lluís Brosa, A. Comerma, J. M. Rossell, and A. D. Dorado, "Architecting an Open-Source IIoT Framework for Real-Time Control and Monitoring in the Bioleaching Industry," *Applied sciences*, vol. 14, no. 1, pp. 350–350, Dec. 2023, doi: https://doi.org/10.3390/app14010350.

[11] Adiva Fiqri Nugraha, H. Kabetta, I Komang Setia Buana, and R Budiarto Hadiprakoso, "Performance and Security Comparison of Json Web Tokens (JWT) and Platform Agnostic Security Tokens (PASETO) on RESTful APIs," Aug. 2023, doi: https://doi.org/10.1109/icocics58778.2023.10277377.

[12] B. Djamaa, M. R. Senouci, H. Bessas, B. Dahmane, and A. Mellouk, "Efficient and Stateless P2P Routing Mechanisms for the Internet of Things," *IEEE Internet of Things Journal*, pp. 1–1, 2021, doi: https://doi.org/10.1109/jiot.2021.3053339.

[13] J. Gómez, Abdelhamid Tayebi, and J. Casado, "On the Use of Websockets to Maintain Temporal States in a Stateless Application," pp. 21–24, Sep. 2020.