JOURNAL
TICOM
TECHNOLOGY OF INFORMATION AND COMMUNICATION

Vol. 9 No. 3, Mei 2021 ISSN : 2302-3252

ASOSIASI PERGURUAN TINGGI INFORMATIKA & ILMU KOMPUTER
(APTIKOM) WILAYAH 3

Sekretariat Redaksi :
Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. 021.5853753 Fax .021.5869225

Implementasi Web Service Menggunakan Json Web Token pada Perusahaan Security

Mahesa Pandu Wicaksana [1)], Dolly Virgian Shaka Yudha Sakti [2)], Dewi Kusumaningsih [3)]

Fakultas Teknologi Informasi, Universitas Budi Luhur [1,2,3)]
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5853752
E-mail: akumahesaa@gmail.com [1)], dolly.virgianshaka@budiluhur.ac.id [2)], dewi.kusumaningsih@budiluhur.ac.id [3)]

Abstrak - Perkembangan jasa sekuriti di Indonesia telah meningkat, PT Mitra Bhakti Nusa adalah salah satu penyedia layanan sekuriti di Indonesia khususnya di daerah Bogor. Sekuriti akan berpatroli dan melakukan absensi secara rutin untuk dilihat aktivitas serta kinerjanya dan sering kali terjadi kesalahan penginputan data karena masih dilakukan secara manual. Kesalahan pengolahan data tersebut biasanya terjadi karena kelalaian sang pengolah data. Untuk memudahkan pengolahan data serta monitoring sekuriti secara tepat, dikembangkanlah aplikasi web servis dengan di implementasikannya RESTful serta aplikasi mobile untuk menunjang semua hal itu. Arsitektur REST merupakan salah satu penjembatan antara web servis dengan aplikasi mobile, salah satu kelemahannya adalah autentikasinya. Untuk menanggulangi masalah sekuriti, di implementasikan sebuah teknologi yang bernama JSON Web Token (JWT) untuk menunjang keamanan transfer data. Sehingga, untuk melayani request dari client diperlukan sebuah akses token yang akan mengidentifikasi client. Penelitian ini menghasilkan sebuah aplikasi web servis beserta aplikasi mobile yang dapat digunakan untuk menunjang kebutuhan tersebut. Hasil penelitian ini menemukan bahwa pengembangan sistem web service beserta aplikasi mobile, pengujian metode, dan analisa program dari aplikasi ini, dapat diambil kesimpulan, bahwa seluruh endpoint yang sudah disediakan untuk client android dapat berjalan dengan baik. Dengan melakukan implementasi web service dengan client android proses pengolahan data menjadi lebih efisien, dan juga lebih akurat dalam pendataannya. Sebelumnya tanpa adanya aplikasi ini, proses pengolahan data manual bisa menimbulkan human error dan juga memakan waktu yang cukup lama tergantung individu yang melakukan pengolahan data, sekarang untuk proses perekapan absen tinggal melakukan export data dari web-admin untuk mengambil laporan dari absensi beserta patrol satpam. Dengan waktu layanan yang mempunyai rata-rata 257 ms, keakuratan data serta kecepatan untuk melakukan rekap data menjadi lebih cepat dan efisien hanya dengan beberapa klik saja.

Kata Kunci: Web Service, Restful, Json Web Token, Monitoring Security, Absen

Abstract – Security services in Indonesia have developed, PT Mitra Bhakti Nusa is one of the security service providers in Indonesia especially in the Bogor area. Security will patrol and perform regular attendance to be seen their activities and performance, and often there is an error in data entry because it is still done manually. Data processing errors usually occur due to negligence of the data processor (admin). To facilitate data processing and proper security (employee) monitoring, a web service application was developed with the implementation of RESTful and a mobile application to support it. REST architecture is one of the bridges between web services and mobile applications, one of the weaknesses is authentication. To overcome this problem, a technology called JSON Web Token was implemented to support data transfer security. So, to serve requests from clients, an access token is needed to identify the client. This research produces a web service application along with a mobile application that can be used to support these needs. The results of this study found that with the development of web service systems along with mobile applications, testing methods, and program analysis of this application, it can be concluded that all endpoints provided for android clients can run well. By implementing a web service with an android client, the data processing process becomes more efficient, and also more accurate in data collection. Previously without this application, manual data processing could cause a human error and also took a long time depending on the individual processing the data, now for the attendance recording process admin can export data from the web to retrieve reports from attendance and security patrols. With an average service time of 257 ms, data accuracy and time to data recap is faster and more efficient with just a few clicks.

Keywords: Web Service, Restful, Json Web Token, Security Monitoring, Attendance

I. PENDAHULUAN

Sektor Pariwisata, hotel, garmen dan ritel biasanya membutuhkan jasa pengamanan dikenal satpam atau sekuriti. Sejak Covid-19 melanda maret hingga saat ini, sektor tersebut goyang dan berdampak pada kebutuhan jasa sekuriti. Agoes Dermawan Ketua BPP Asosiasi Badan Usaha Jasa Pengamanan Indonesia (Abujabi) menjelaskan tidak sedikit anggota sekuriti di anggota Abujabi yang di rumahkan. Ia mengungkapkan tagihan yang diajukan ke klien, mundur akibat tekanan covid-19. Di tambah, perjuangan melawan covid, kebutuhan alat protokol kesehatan haru disediakan oleh pihaknya[1].

PT Mitra Bhakti Nusa Sekuriti merupakan salah satu perusahaan yang bergerak di bidang jasa keamanan sekuriti. Jasa keamanan dalam konteks aktifitas dapat berarti perusahaan swasta yang memiliki kegiatan memberikan jasa atau keahlian dalam bidang keamanan. Keahlian dimaksud dapat berupa penyediaan peralatan ataupun penjagaan sekuriti secara pribadi. Semua tentang usaha dan cara menjaga keselamatan orang atau barang. Pada proses bisnis yang berjalan saat ini terdapat beberapa permasalahan dalam pengelolaan informasi, misalnya sering terjadi perbedaan data antar bagian terkait dengan data laporan absensi petugas keamanan, laporan kejadian aktifitas, serta kesalahan input pada sistem yang diakibatkan oleh kesalahan manusia, Hal tersebut dikarenakan penginputan data dilakukan dengan proses penginputan manual form yang relatif sederhana dan memakan waktu yang relatif lambat, yaitu kurang lebih satu hari untuk satu penanganan proses laporan[2].

PT Mitra Bhakti Nusa Sekuriti salah satu perusahaan yang bergerak di bidang jasa keamanan. Jasa keamanan adalah bisnis yang mengedepankan kepercayaan dimana para petugas keamanan diberi kewenangan untuk menjaga sebuah gedung, rumah, atau lainnya. Maka pada proses bisnis yang berjalan saat ini terdapat beberapa permasalahan dalam pengelolaan informasi. Adapun penyebab munculnya permasalahan tersebut karena sering terjadinya kelalaian yang dilakukan oleh bagian tertentu, contohnya petugas keamanan yang dikirim tidak melakukan kegiatannya dengan baik. Apabila kita mampu mengelola informasi dengan baik maka kapan dan dimanapun kita akan memperoleh hasil yang tepat dan akurat.

Web service adalah suatu sistem perangkat lunak yang dirancang untuk mendukung interoperabilitas dan interaksi antar sistem pada suatu jaringan[3]. Web service digunakan sebagai suatu fasilitas yang disediakan oleh suatu web site untuk menyediakan layanan (dalam bentuk informasi) kepada sistem lain, sehingga sistem lain dapat berinteraksi dengan sistem tersebut melalui layanan-layanan (service) yang disediakan oleh suatu sistem yang menyediakan web service[4]. Web service juga diartikan sebagai sebuah antar muka yang menggambarkan sekumpulan operasi-operasi yang dapat diakses melalui jaringan dalam bentuk XML.

Teknologi web service menyediakan layanan-layanan pada suatu website, dimana layanan-layanan tersebut berupa objek dan metode yang memiliki tujuan untuk memfasilitasi sistem lain agar dapat berkomunikasi tanpa terikat platform dan tanpa terikat bahasa pemrograman[5]. Artinya, dengan adanya web service, maka sistem dengan platform dan atau sistem dengan bahasa pemrograman yang berbeda dapat saling berinteraksi. Dalam membangun webservice, terdapat tiga metode yang dapat digunakan, antara lain SOAP, XML-RPC, dan REST. Dalam penelitian ini, web service digunakan untuk menyediakan layanan berupa objek dan metode-metode sehingga aplikasi android pada mobile phone yang menggunakan bahasa pemrograman java dapat berinteraksi dengan database yang menggunakan bahasa pemrograman SQL dan HTTP sebagai platform dasar dari web service.

Android adalah sistem operasi mobile berbasi open source dari linux yang dikembangkan oleh Google Android.Inc. Gooogle menginginkan Android untuk menjadi sistem operasi open source dan gratis, kebanyakan code Android dirilis di bawah lisensi open source apache yang barcode android

Penelitian ini bertujuan untuk menyelesaikan masalah pada PT Mitra Bhakti Nusa dengan cara mengimplementasikan metode keamanan menggunakan JSON Web Token pada sistem web service yang akan digunakan untuk autentikasi. Diharapkan dengan adanya penelitian ini keamanan transfer data serta kecepatan, ketepatan dan efisiensi pengolahan data menjadi lebih baik dari sebelumnya.

II. METODOLOGI PENELITIAN

Untuk dapat memecahkan permasalahan maka penelitian ini mengimplementasikan web service, dengan tahap-tahap sebagai berikut.

Gambar 1. Tahap Penelitian [7].

Pada Gambar 1, menjelaskan bahwa metode penelitian yang digunakan. Studi literatur berupa memperoleh informasi dari penelitian-penelitian sebelumnya dengan cara mempelajari metode-metode yang digunakan seperti JSON Web Token, Web Service, RESTful API, dan sebagainya yang berhubungan dengan penelitian. Analisis permasalahan dilakukan untuk menentukan kebutuhan sistem. Penerapan metode-metode seperti JSON Web Token dalam RESTful API web service. Perancangan sistem android dengan menggunakan model sistem yang sudah dibuat. Evaluasi sistem dengan melakukan uji coba untuk mengetahui stabilitas dan performa sistem yang telah dibuat. Pengujian ini dilakukan untuk mengetahui fungsionalitas dari software yang telah dibuat dengan menggunakan metode pengetesan black box testing. Black box testing adalah metode pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak.

REST Web Service adalah bagian dari HTTP dimana menyediakan antarmuka yang seragam seperti membuat, mengambil, memperbarui, menghapus dan memanipulasi sumber daya dengan pertukaran representasi. REST bersifat stateless yang artinya pesan tidak bergantung pada keadaan percakapan. Arsitektur REST digunakan untuk memanipulasi data pada sebuah sistem dengan menggunakan metode protokol. Data diidentifikasi dengan Uniform Resource Locator (URL) untuk digunakan sebagai antar muka dalam memanipulasi sumber daya. Dalam arsitektur REST kembalian sumber daya dapat berupa format XML, HTML, JSON ataupun format yang lain. Dengan mengunakan protocol HTTP/HTTPS yang bersifat stateless, arsitektur REST ditujukan untuk performance, reliability dan scalability[6].

Metode yang digunakan dalam REST diantaranya: GET untuk mendapatkan sumber daya, POST digunakan untuk membuat sumber daya baru dan metode PUT digunakan untuk memperbarui sumber daya berdasarkan sumber daya. Sedangkan metode DELETE digunakan untuk menghapus sumber daya atau kumpulan sumber daya[5].

Pada penilitian ini, diimplementasikan beberapa endpoint yang akan digunakan oleh client android yang terlihat pada Tabel 1.

Tabel 1. Daftar endpoint Web Service.

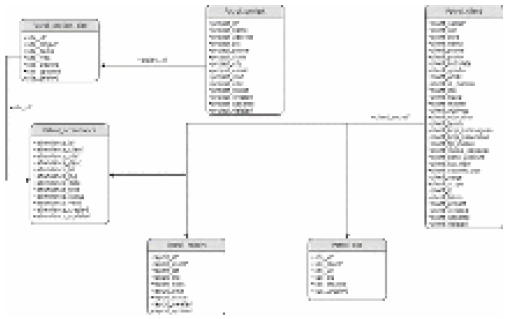
Service Name	*Method*	*Path*	*Parameter*	*Header*
User authenticate	*POST*	*/v1/oauth/authorize*	*Username, password*	
User token refresh	*POST*	*/v1/oauth/token*	*Grant_type, client_secret, code*	
User logout	*POST*	*/v1/oauth/logout*		*Authorization: Bearer JWT Token*
User attendance	*POST*	*/v1/patrol/attendance*	*Attendance_type, attendance_site, attendance_lat, attendance_lng*	*Authorization: Bearer JWT Token*
User patrol report	*POST*	*/v1/patrol/report*	*Report_lat, Report_lng, Report_desc, Report_status, Report_data[]*	*Authorization: Bearer JWT Token*
User checkpoint attendance	*POST*	*/v1/patrol/attendance*	*Attendance_site, attendance_type, attendance_lat, attendance_lng, attendance_desc, attendance_status, attendance_data[]*	*Authorization: Bearer JWT Token*
User SOS Signal	*POST*	*/v1/patrol/sos*	*Sos_lat, sos_lng*	*Authorization: Bearer JWT Token*
User activity history list	*GET*	*/v1/patrol/history*		*Authorization: Bearer JWT*

Service Name	*Method*	*Path*	*Parameter*	*Header*
				Token

Pada Tabel 1, terlihat daftar endpoint yang disediakan oleh web service. Endpoint tersebut memiliki fungsi dan inputan yang berbeda. Setiap endpoint yang membutuhkan header akan diberikan sebuah JWT Token sebagai Bearer Token-nya. Dengan dikirimnya JWT Token sebagai Bearer Token, web service dapat dengan mudah mengidentifikasi siapa pengirim request tersebut.

III. Hasil dan Pembahasan

Dari segala kebutuhan yang telah diambil dari lokasi penelitian, didapatkan hasil berupa basis data yang dapat memenuhi semua kebutuhan untuk layanan web service yang disajikan dalam bentuk Logical Record Structure (LRS) pada Gambar 2.



Gambar 2. Rancangan Logical Record Structure (LRS).

Pada gambar 2, terlihat struktur dari basis data yang digunakan untuk memenuhi kebutuhan. Basis data tersebut terdiri dari beberapa tabel yaitu patrol_project, patrol_client, patrol_project_site, patrol_attendance, patrol_report, dan patrol_sos.

Pembuatan basis data adalah salah satu tahap awal dalam penelitian ini, setelah itu adalah pengimplementasian autentikasi dengan JSON Web Token pada web service. Setiap route endpoint yang membutuhkan validasi token tersebut akan melewati sebuah middleware yang akan memvalidasi keabsahan token tersebut. Pengetesan yang dilakukan untuk implementasi token dilakukan dengan percobaan login kedalam aplikasi yang nantinya akan memberikan output berupa data user beserta token untuk autentikasi pada request selanjutnya. Pengujian dilakukan pada endpoint /v1/oauth/authorize menggunakan metode POST dengan kredensial username satpam menghasilkan respon berhasil dengan waktu eksekusi 209 ms, menghasilkan respon berupa informasi user satpam dengan token sebagai berikut:

“eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI0MDQxMjYwNmYzZDExZTliMTkwMTVmYjkxYWI0NmZhZHgiLCJpc3MiOiJodHRwczovL21ibi5yb25hZGlnaXRlY2guY29tL2FwaS92MS9vYXV0aC9hdXRob3JpemUiLCJpYXQiOjE2MTI4NzkxNTIsImV4cCI6MTYxMjk2NTU1MiwibmJmIjoxNjEyODc5MTUyLCJqdGkiOiJ3QlhlV00wTnNLSW5YWmNPIn0.rlWE-ypJJzcONbfKOL6MLZjDzlgntYlZFqX-9IbPnnc”.

Pada pengujian di atas, eksekusi fungsi login dilakukan dengan autentikasi menggunakan kredensial yang digunakan untuk masuk kedalam aplikasi. Apabila kredensial tersebut valid, maka akan diberikan respon berupa informasi user terkait serta akses token JWT untuk user tersebut. Apabila kredensial tidak valid, maka akan muncul respon “invalid credentials”. Untuk menghindari hal tersebut, web-admin harus melakukan penambahan user terlebih dahulu.

Pada pengujian fungsi login didapatkan juga data-data lainnya berupa informasi user yang terlihat pada Gambar 3.

Gambar 3. Output fungsi login pada endpoint /v1/oauth/authorize.

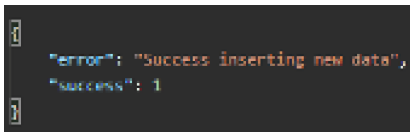
Setelah melakukan pengujian pada endpoint yang digunakan untuk melakukan generate token serta mengambil informasi user. Dilakukan juga pengujian terhadap endpoint-endpoint lainnya yang disediakan oleh layanan web service.

Gambar 4. Output fungsi refresh token pada endpoint /v1/oauth/token.

Pada Gambar 4, pengujian dilakukan menggunakan metode POST pada endpoint /v1/oauth/token untuk melakukan refresh terhadap token JWT agar tidak kadaluarsa dan mengambil data pengguna untuk menghindari data yang tidak sinkron. Pengujian berhasil dengan waktu 185 ms dan menghasilkan ukuran file sebesar 2.0 kb.

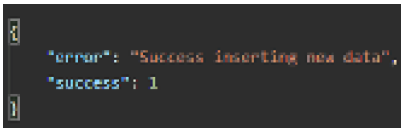
Gambar 5. Output fungsi logout pada endpoint /v1/oauth/logout.

Pada Gambar 5, pengujian dilakukan menggunakan metode POST pada endpoint v1/oauth/logout untuk menghapus sesi pengguna beserta melakukan penghapusan token JWT. Pengujian berhasil dilakukan dengan waktu 168 ms, dan menghasilkan ukuran file sebesar 788 B.



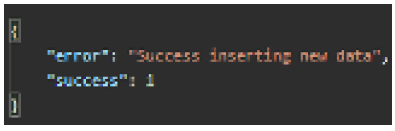
Gambar 6. Output fungsi absensi masuk pada endpoint /v1/patrol/attendance.

Pada Gambar 6, pengujian dilakukan menggunakan metode POST pada endpoint /v1/patrol/attendance untuk melakukan absensi masuk maupun keluar. Pengujian berhasil dilakukan dengan waktu 410 ms, dan menghasilkan ukuran file sebesar 810 B.



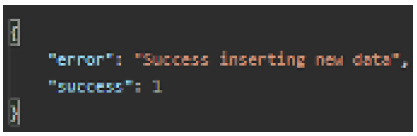
Gambar 7. Output fungsi laporan patroli pada endpoint /v1/patrol/report.

Pada Gambar 7, pengujian dilakukan menggunakan metode POST pada endpoint /v1/patrol/report untuk membuat laporan patroli. Pengujian berhasil dilakukan dengan waktu 357 ms, dan menghasilkan ukuran file sebesar 629 B.



Gambar 8. Output fungsi absensi patroli pada endpoint /v1/patrol/attendance.

Pada Gambar 8, pengujian dilakukan menggunakan metode POST pada endpoint /v1/patrol/attendance untuk melakukan laporan patrol per checkpoint yang sudah ditentukan. Pengujian berhasil dilakukan dengan waktu 454 ms, dan menghasilkan ukuran file sebesar 810 B.



Gambar 9. Output fungsi sinyal darurat pada endpoint /v1/patrol/sos.

Pada Gambar 9, pengujian dilakukan menggunakan metode POST pada endpoint /v1/patrol/sos untuk melakukan pengiriman sinyal darurat. Pengujian berhasil dilakukan dengan waktu 146 ms, dan menghasilkan ukuran file sebesar 629 B.

Gambar 10. Output fungsi riwayat user pada endpoint /v1/patrol/history.

Pada Gambar 10, pengujian dilakukan menggunakan metode metode GET pada endpoint /v1/patrol/history untuk mendapatkan riwayat aktivitas pengguna. Pengujian berhasil dilakukan dengan waktu 133 ms, dan menghasilkan ukuran file sebesar 1.16 KB.

Setelah semua endpoint telah diuji, tahap selanjutnya adalah implementasi pada Operating System Android yang dimana akan digunakan sebagai client pengirim request ke web service. Berikut ini adalah beberapa tangkapan layar beserta penjelasannya dari aplikasi android yang telah dibuat dalam penelitian ini.

Gambar 11. Tangkapan Layar Login

Gambar 11, merupakan tangkapan layar dari form login. User akan memasukan username dan password pada form login untuk masuk kedalam aplikasi. Web admin akan membuat akun baru dan mendistribusikannya ke user terkait untuk masuk kedalam aplikasi. Pada fitur ini, metode yang di implementasi adalah POST ke endpoint /v/1/oauth/authorize.

Gambar 12. Tangkapan Layar Dashboard

Gambar 12, berisi navigasi untuk menu menu lainnya, user dapat melihat riwayat aktivitas dengan card yang tersedia atau bisa menekan tombol riwayat untuk melihat secara full-page. Pada halaman ini, dilakukan proses pengambilan data riwayat dengan melakukan metode GET pada endpoint /v1/patrol/history.

Gambar 13. Tangkapan Layar Buat Laporan

Pada Gambar 13, halaman ini berisi sebuah form untuk melakukan sebuah laporan tanpa harus absen atau melakukan scan qr-code. Pada halaman ini jika user melakukan submit laporan maka akan dilakukan proses menggunakan metode POST pada endpoint /v1/patrol/report.

Gambar 14. Tangkapan Layar Absen Masuk atau Keluar

Gambar 14, memperlihatkan halaman untuk absen masuk maupun keluar, halaman ini diakses setelah user melakukan scanning terhadap qr-code. User harus mengambil beberapa foto untuk melakukan absensi masuk maupun keluar. Metode POST pada endpoint /v1/patrol/attendance digunakan pada halaman ini saat user melakukan submit.

Setelah pembuatan web service beserta aplikasi android, sistem juga dilakukan pengujian menggunakan metode blackbox. Hasilnya akan ditemukan berapa lama waktu yang dibutuhkan dalam menangani satu request. Semua evaluasi tersebut tersaji dalam Tabel 2.

Tabel 2. Analisa Pengujian Waktu Layanan Web Service

Proses	*Deskripsi*	*Waktu*
POST /v1/oauth/authorize	*Masuk kedalam aplikasi*	*209 ms*
POST /v1/oauth/token	*Memperbaharui akses token*	*185 ms*
POST /v1/oauth/logout	*Keluar dari aplikasi*	*168 ms*
POST /v1/patrol/attendance	*Melakukan absen masuk atau keluar*	*410 ms*
POST /v1/patrol/report	*Melakukan laporan patroli*	*357 ms*
POST /v1/patrol/attendance	*Melakukan absensi patrol di checkpoint*	*454 ms*

Proses	*Deskripsi*	*Waktu*
POST /v1/patrol/sos	*Mengirimkan sinyal darurat*	*146 ms*
GET /v1/patrol/history	*Melihat daftar riwayat aktivitas pengguna*	*133 ms*
	Rata-rata Waktu	*257 ms*

Setelah dilakukan tahap pengujian aplikasi dengan metode Blackbox, ditemukan hasil berupa satuan waktu dalam proses autentikasi hingga seluruh fitur dan proses yang telah disediakan.

Seluruh layanan yang disediakan oleh web service berfungsi dengan baik, dengan proses autentikasi pengguna dapat diselesaikan dalam waktu rata-rata 220ms. Sebagaimana yang telah dijabarkan pada Tabel 1, seluruh endpoint dengan metode POST maupun GET, yang telah dilakukan pengujian untuk mendapatkan waktu proses rata-rata yaitu dengan waktu rata-rata selama 257 ms. Selain dilakukannya pengujian waktu, dilakukan juga pengujian terhadap fungsi aplikasi yang telah disediakan. Hasil dari pengujian fungsi aplikasi dapat dilihat hasilnya pada Tabel 3.

Tabel 3. Evaluasi Pengujian Black Box Untuk Fungsi Aplikasi

Aktifitas	*Input*	*Output*	Status
User melakukan *login*	*Username, password*	Jika *username* dan *password* dinyatakan valid maka akan diberikan respon berupa akses token beserta dengan data *user* Jika *username* atau *password* dinyatakan tidak valid maka akan diberikan respon berupa pesan *error invalid credentials*	Valid
User melakukan *refresh token*	*Grant_type, code, client_secret*	Jika semua inputan tersebut valid, maka akan diberikan respon berupa akses token yang baru beserta dengan data *user* Jika *client_secret* tidak valid, akan diberikan respon berupa pesan *error invalid credentials*	Valid
User melakukan *logout*	-	Jika akses token *user* valid, maka akan diberikan respon bahwa *logout* sukses	Valid
		Jika akses token *user* tidak valid, maka akan diberikan respon berupa pesan *error token invalid*	
User melakukan absensi masuk atau keluar	*Attendance_type, attendance_site, attendance_lat, attendance_lng*	Jika semua inputan diisi oleh *user* dan data tersebut valid, maka akan diberikan respon sukses Jika salah satu field tidak di isi atau data tersebut tidak valid maka akan diberikan respon *error* berupa *invalid*	Valid
User melakukan laporan patroli	*Report_lat,* *Report_lng,* *Report_desc,* *Report_status, Report_data []*	Jika semua inputan diisi oleh *user* dan data tersebut valid, maka akan diberikan respon sukses Jika salah satu field tidak di isi atau data tersebut tidak valid maka akan diberikan respon *error* berupa *invalid*	Valid
User melakukan absensi patrol di *checkpoint*	*Attendance_site, attendance_type, attendance_lat, attendance_lng, attendance_desc, attendance_status, attendance_data[]*	Jika semua inputan diisi oleh *user* dan data tersebut valid, maka akan diberikan respon sukses Jika salah satu field tidak di isi atau data tersebut tidak valid maka akan diberikan respon *error* berupa *invalid*	Valid
User melakukan pengiriman sinyal darurat	*Sos_lat, sos_lng*	Jika semua inputan diisi oleh *user* dan data tersebut valid, maka akan diberikan respon sukses Jika salah satu field tidak di isi atau data tersebut tidak valid maka akan diberikan respon *error* berupa *field* tersebut harus di isi	Valid
User melakukan pengambilan data riwayat	-	Jika semua inputan tersebut valid, maka akan diberikan respon berupa data riwayat *user* Jika akses token *user* tidak valid, akan diberikan respon berupa pesan *error token invalid* atau *token expired*	Valid

Pada Tabel 3, terlihat dengan jelas dan dapat disimpulkan bahwa hasil evaluasi dari fungsi aplikasi yang telah dikembangkan memiliki fungsi-fungsi yang berjalan dengan baik tanpa hambatan.

IV. KESIMPULAN

Berdasarkan pengembangan sistem web service beserta aplikasi mobile, pengujian metode, dan analisa program dari aplikasi ini, penulis mempunyai beberapa kesimpulan, yaitu:

- Seluruh endpoint yang disediakan oleh web service untuk dikonsumsi oleh client dapat berfungsi dan berjalan dengan baik tanpa masalah.
- Dengan melakukan implementasi web service dan didampingi dengan client android, proses pengolahan data menjadi lebih efisien dan juga lebih akurat dalam pendataannya. Sebelum adanya aplikasi ini, pengolahan data bisa memicu terjadinya human error dalam penginputan serta pengolahan dan juga memakan waktu yang cukup lama dalam prosesnya tergantung dari keahlian individu yang melakukan pengolahan. Sekarang, dengan adanya fitur export data absensi dan laporan satpam di web-view untuk web-admin proses perekapan data menjadi lebih efisien dan mudah.
- Waktu layanan web service mempunyai rata-rata waktu 257 ms, keakuratan data serta kecepatan untuk melakukan rekap data menjadi lebih cepat dan efisien hanya dengan beberapa klik saja.
- Keamanan aplikasi bisa menjadi lebih terjamin karena server dapat mengidentifikasi siapa pengirim request karena diimplementasikannya JSON Web Token (JWT) untuk autentikasi.

V. DAFTAR PUSTAKA

[1] Wiyanto, “Usaha Jasa Pengamanan Menjerit, Security Banyak Dirumahkan,” industrycoid, 2020. .

[2] M. R. Royani and W. Arief, “Implementasi Web Service pada Perusahaan Logistik menggunakan JSON Web Token dan Algoritma Kriptografi RC4,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 4, no. 3, 2020, doi: 10.29207/resti.v4i3.1952.

[3] A. Hibsy and A. Wibowo, “Implementasi Fitur Keamanan dengan JSON Web Tokendan Fitur Geo-taggingpada AplikasiWeb ServiceTraining From Home,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 4, no. 4, 2020, doi: 10.29207/resti.v4i4.1973.

[4] P. Painem and H. Soetanto, “Sistem Presensi Pegawai Berbasis Web Service Menggunakan Metode Restfull Dengan Keamanan JWT Dan Algoritma Haversine,” Fountain Informatics J., vol. 5, no. 3, 2020, doi: 10.21111/fij.v5i3.4906.

[5] A. Rahmatulloh, H. Sulastri, and R. Nugroho, “Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512,” J. Nas. Tek. Elektro dan Teknol. Inf., vol. 7, no. 2, 2018, doi: 10.22146/jnteti.v7i2.417.

[6] B. Satria, A. Kusyanti, and W. Yahya, “Implementasi Algoritme Blake2s pada JSON Web Token (JWT) sebagai Algoritme Hashing untuk Mekanisme Autentikasi Layanan REST-API,” J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya, vol. 2, no. 12, 2018.