

**IMPLEMENTASI
SECURE WEBSOCKET DAN CLIENT AUTHENTICATION
UNTUK APLIKASI SISTEM KONTROL ROBOT BERBASIS ROS 1**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

AHMAD FEBRIANTO

18.83.0195

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

**IMPLEMENTASI
SECURE WEBSOCKET DAN CLIENT AUTHENTICATION
UNTUK APLIKASI SISTEM KONTROL ROBOT BERBASIS ROS 1**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

AHMAD FEBRIANTO

18.83.0195

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

HALAMAN PERSETUJUAN
SKRIPSI

IMPLEMENTASI
SECURE WEBSOCKET DAN CLIENT AUTHENTICATION
UNTUK APLIKASI SISTEM KONTROL ROBOT BERBASIS ROS 1

yang disusun dan diajukan oleh

Ahmad Febrianto

18.83.0195

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Agustus 2022

Dosen Pembimbing,

Wahyu Sukestyastama Putra, S.T., M.Eng

NIK. 190302328

HALAMAN PENGESAHAN
SKRIPSI
IMPLEMENTASI
SECURE WEBSOCKET DAN CLIENT AUTHENTICATION
UNTUK APLIKASI SISTEM KONTROL ROBOT BERBASIS ROS 1

yang disusun dan diajukan oleh

Ahmad Febrianto
18.83.0195

Telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Agustus 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Muhammad Kopravi, S.Kom, M.Eng
NIK. 190302454

Senie Destya, M.Kom.
NIK. 190302312

Wahyu Sukestyastama Putra, S.T., M.Eng
NIK. 190302328

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ahmad Febrianto
NIM : 18.83.0195

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Secure Websocket dan Client Authentication Untuk Aplikasi Sistem Kontrol Robot Berbasis Ros 1

Dosen Pembimbing : Wahyu Sukestyastama Putra, S.T., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Juli 2022

Yang Menyatakan,



Ahmad Febrianto

HALAMAN PERSEMBAHAN

Saya persembahkan skripsi ini secara khusus kepada kedua orang tua tercinta dan segenap keluarga kecil saya yang telah memberi dukungan tanpa batas dari awal sampai akhir studi saya di Universitas Amikom Yogyakarta.



KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah Subhanahu Wata'ala atas segala nikmat dan karunia sehingga penulis dapat menyelesaikan rangkaian penulisan skripsi ini dengan baik. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Ilmu Komputer Prodi Teknik Komputer Fakultas Ilmu komputer Universitas Amikom Yogyakarta.

Penulisan skripsi ini mengalami banyak rintangan, salah satu yang terbesar adalah pemilihan topik penelitian. Hal ini menjadi dilema bagi penulis selama berbulan-bulan. Pada akhirnya penulis mendapatkan ilham tentang ide penelitian skripsi yang tepat. Ide penelitian ini kemudian melahirkan judul penelitian “Implementasi Keamanan Terhadap Aplikasi Sistem Kontrol Robot Berbasis ROS 1”.

Adanya topik penelitian tentu bukan sebuah jaminan selesainya sebuah skripsi. Penulis bersyukur karena selama pengerjaan skripsi, penulis memiliki rekan-rekan dan dosen pembimbing yang sangat suportif. Dukungan dan dorongan dari mereka sangat berarti bagi penulis di dalam menyelesaikan penelitian dan penulisan naskah skripsi ini. Penulis ingin berterima kasih secara khusus kepada Bapak Wahyu Sukestyastama Putra, S.T., M.Eng selaku dosen pembimbing, serta kepada seluruh rekan-rekan sekelas yang tidak dapat penulis sebutkan namanya satu persatu.

Sleman, 20 Juli 2022

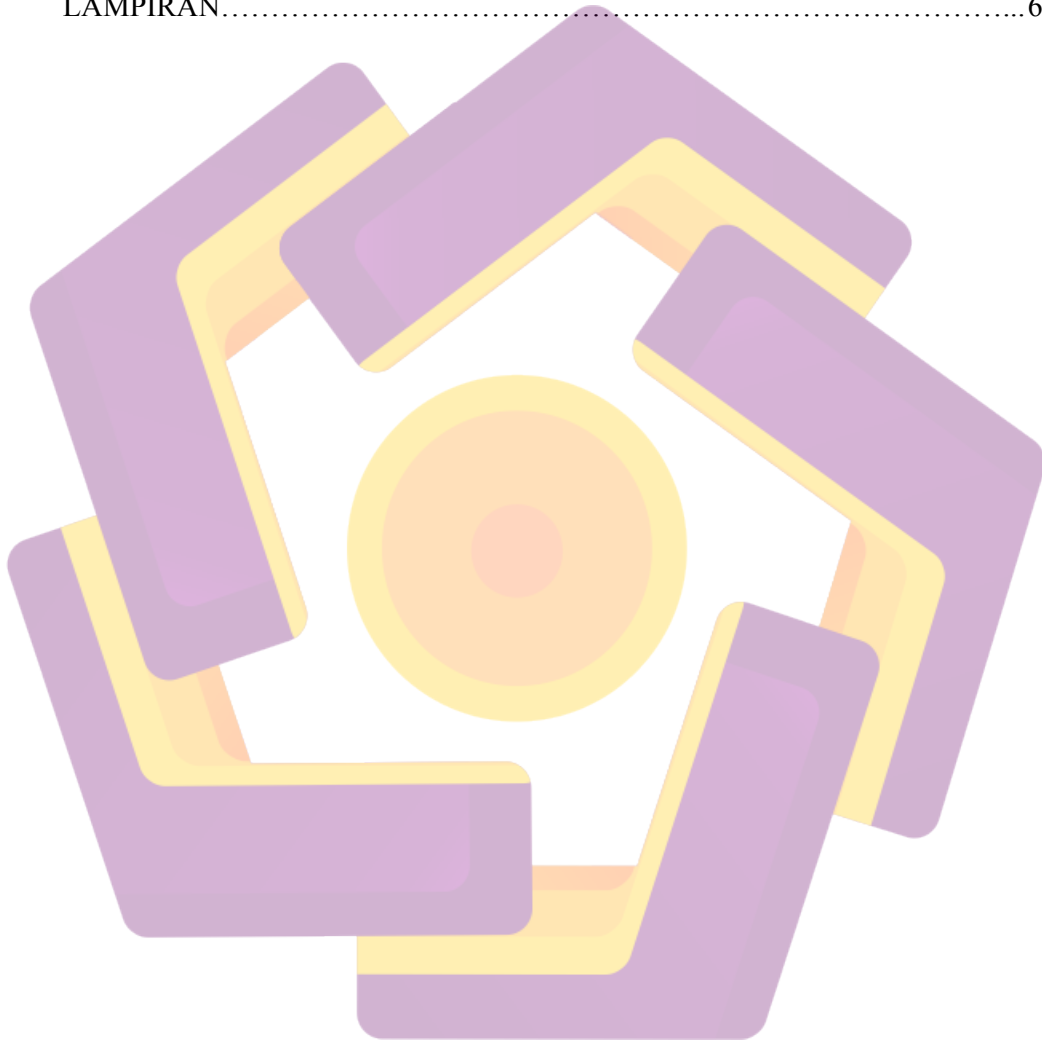
Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN SKRIPSI.....	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	iii
HALAMAN PERSEMBAHAN.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vi
DAFTAR TABEL.....	vi
DAFTAR GAMBAR.....	viii
DAFTAR LAMPIRAN.....	ix
INTISARI.....	x
ABSTRACT.....	xi
BAB I PENDAHULUAN.....	1
Latar Belakang.....	1
Perumusan masalah.....	2
Tujuan Penelitian.....	2
Batasan Masalah.....	2
Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	4
Penelitian Terkait.....	4
Kebaruan Penelitian.....	8
Metode Secure Websocket.....	9
Metode Client Authentication.....	10
Landasan Teori.....	11
Robotic Operating System (ROS).....	11
Rosbridge Websocket Server.....	12
Websocket.....	12

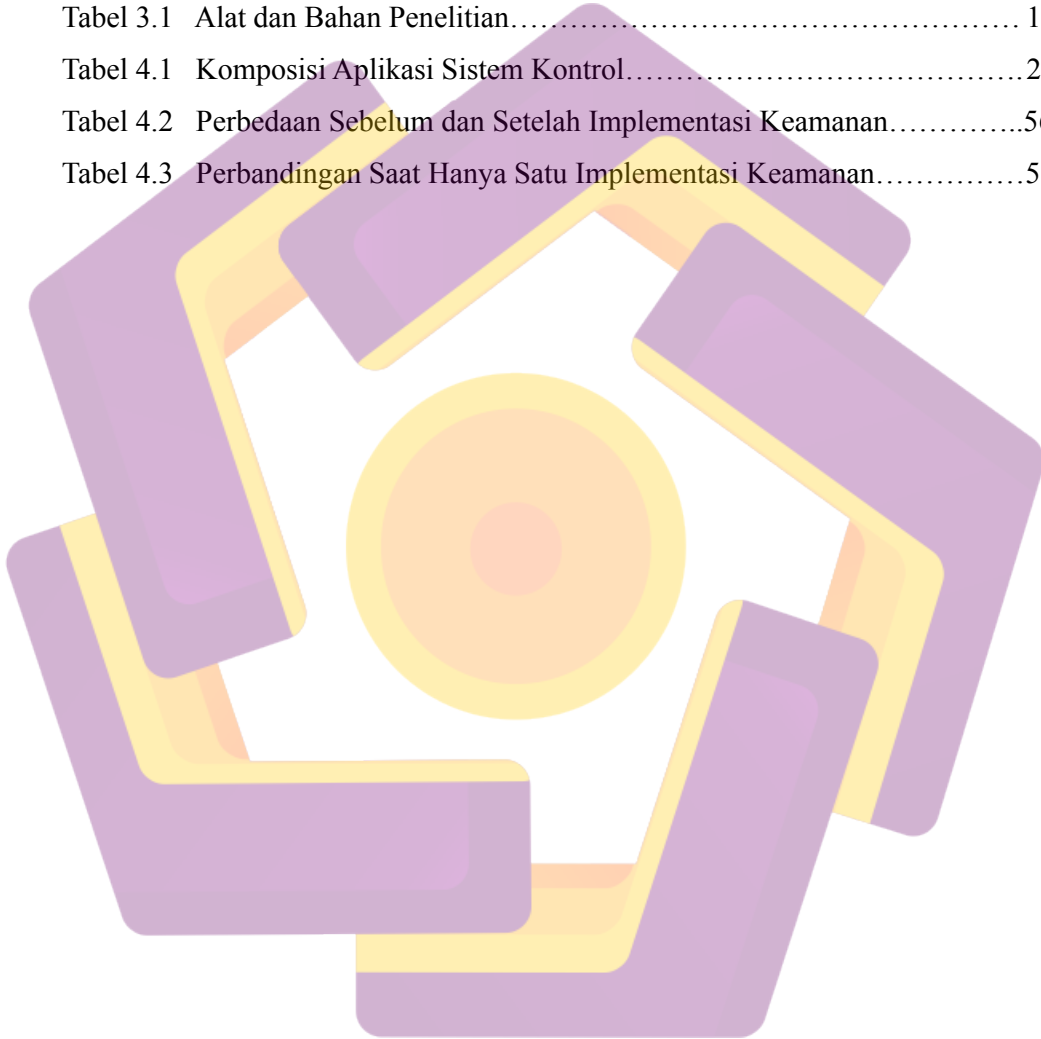
Secure Websocket.....	13
Client Authentication.....	14
Transport Layer Security (TLS)	14
Rosauth.....	14
Message Authentication Code (MAC)	15
Packet.....	16
Aplikasi Sistem Kontrol.....	16
BAB III METODOLOGI PENELITIAN.....	17
Alat dan Bahan Penelitian.....	17
Perangkat Keras.....	18
Perangkat Lunak.....	18
Langkah Penelitian.....	20
Studi Literatur.....	21
Perancangan Sistem.....	21
Implementasi Keamanan.....	21
Pengujian Keamanan.....	21
Analisa Hasil Pengujian.....	21
BAB IV HASIL DAN PEMBAHASAN.....	22
Rancangan Sistem.....	22
Robot.....	22
Client.....	26
Attacker.....	33
Implementasi Keamanan.....	33
Implementasi Secure Websocket.....	33
Implementasi Client Authentication.....	39
Pengujian Keamanan.....	43
Pengujian Secure Websocket.....	43
Pengujian Client Authentication.....	52
Analisa Hasil Pengujian Keamanan.....	56

BAB V KESIMPULAN DAN SARAN.....	58
Kesimpulan.....	58
Saran.....	58
DAFTAR PUSTAKA.....	59
LAMPIRAN.....	61



DAFTAR TABEL

Tabel 2.1	Daftar Penelitian Dengan Implementasi Keamanan.....	7
Tabel 2.2	Hak Cipta Terkait.....	9
Tabel 2.3	Perbedaan Client Authentication dan User Authentication.....	10
Tabel 3.1	Alat dan Bahan Penelitian.....	17
Tabel 4.1	Komposisi Aplikasi Sistem Kontrol.....	27
Tabel 4.2	Perbedaan Sebelum dan Setelah Implementasi Keamanan.....	56
Tabel 4.3	Perbandingan Saat Hanya Satu Implementasi Keamanan.....	57



DAFTAR GAMBAR

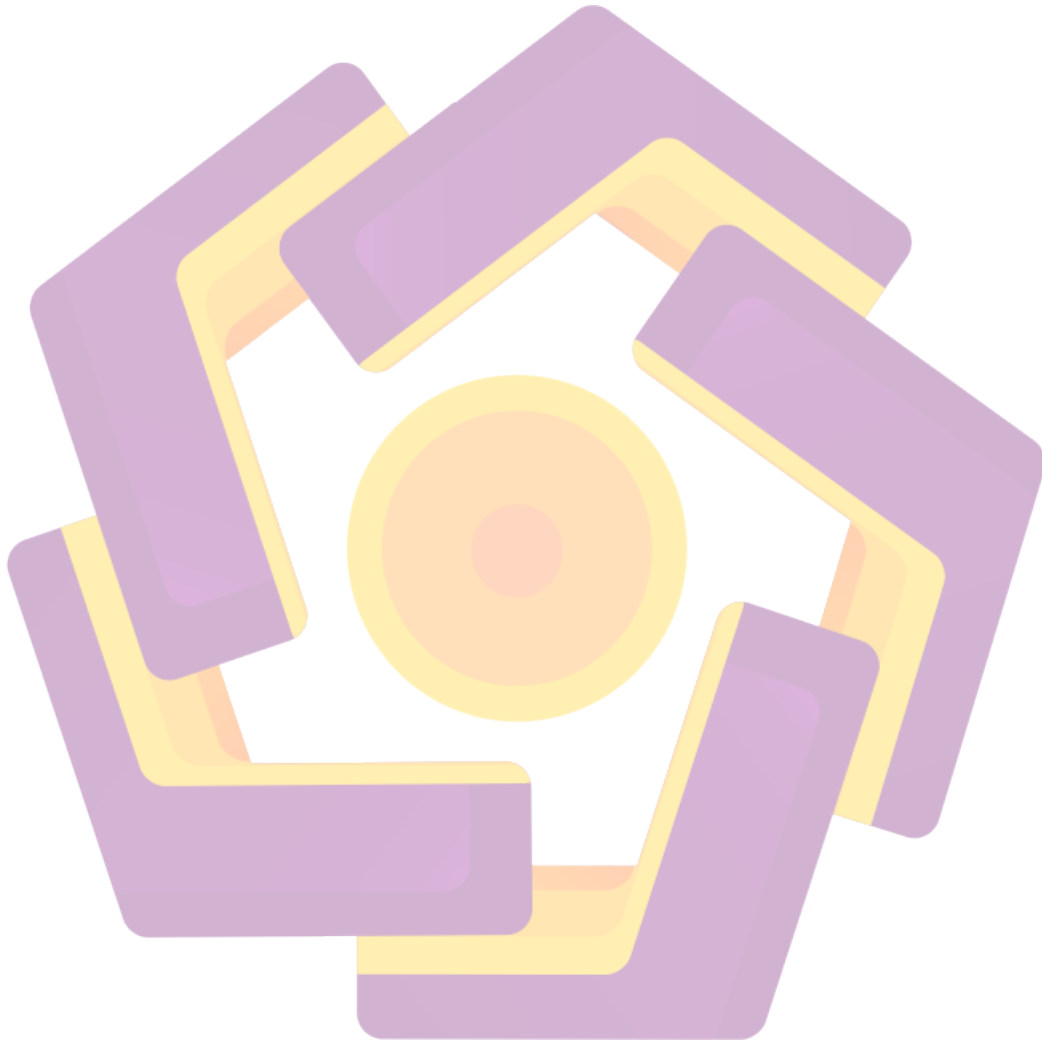
Gambar 2.1	Arsitektur Aplikasi Penelitian [3]	4
Gambar 2.2	Arsitektur Aplikasi Penelitian [4]	5
Gambar 2.3	Arsitektur Aplikasi Penelitian [5]	6
Gambar 2.4	Arsitektur Aplikasi Penelitian [6]	6
Gambar 2.5	Websocket vs HTTP.....	13
Gambar 2.6	Perbedaan Websocket dan Secure Websocket	13
Gambar 2.7	Cara Kerja TLS.....	14
Gambar 2.8	Cara Kerja Message Authentication Code.....	15
Gambar 3.1	Diagram Alur Penelitian.....	20
Gambar 4.1	Topologi Sistem Penelitian	22
Gambar 4.2	Denah Hubungan ROS, Gazebo, dan Turtlebot 3.....	23
Gambar 4.3	Daftar Node ROS Dalam Penelitian	24
Gambar 4.4	Potongan Kode File Launch.....	24
Gambar 4.5	Perintah Untuk Menjalankan File Launch.....	25
Gambar 4.6	Tampilan Robot Turtlebot 3 di Gazebo.....	25
Gambar 4.7	Skema Komunikasi Rosbridge dan Client.....	26
Gambar 4.8	Tampilan Aplikasi Sistem Kontrol	27
Gambar 4.9	Tampilan Komponen Connection.....	29
Gambar 4.10	Potongan Kode Komponen Connection.....	29
Gambar 4.11	Tampilan Status Connected.....	30
Gambar 4.12	Tampilan Status Disconnected.....	30
Gambar 4.13	Fitur Visualisasi Map dan Robot.....	30
Gambar 4.14	Tombol Send dan Cancel Goal.....	31
Gambar 4.15	Pergerakan Robot Setelah Menerima Goal.....	31
Gambar 4.16	Fitur Joystick.....	32
Gambar 4.17	Fitur Pengaturan Kecepatan.....	32

Gambar 4.18	Fitur Logs.....	33
Gambar 4.19	Perintah Pembuatan Private Key.....	34
Gambar 4.20	Output Perintah Pembuatan Private Key.....	34
Gambar 4.21	Perintah Pembuatan CSR.....	34
Gambar 4.22	Output Perintah Pembuatan CSR.....	35
Gambar 4.23	Perintah Penandatanganan Certificate.....	35
Gambar 4.24	Output Perintah Penandatanganan Certificate.....	36
Gambar 4.25	Rosbridge Sebelum Implementasi Secure Websocket.....	36
Gambar 4.26	Rosbridge Setelah Implementasi Secure Websocket.....	36
Gambar 4.27	URL Dengan Skema WS.....	37
Gambar 4.28	URL Dengan Skema WSS.....	37
Gambar 4.29	Log Koneksi Error Ke Robot.....	37
Gambar 4.30	Security Warning Di Browser.....	38
Gambar 4.31	Tampilan Setelah Accept Risk and Continue.....	38
Gambar 4.32	Perintah Pembuatan Kata Kunci Rahasia.....	39
Gambar 4.33	Penambahan Argumen Authenticate di Rosbridge.....	39
Gambar 4.34	Konfigurasi Rosauth di File Launch.....	40
Gambar 4.35	Tampilan Fungsi Authenticate.....	41
Gambar 4.36	Tampilan Penggunaan Fungsi Authenticate.....	42
Gambar 4.37	Komponen Connection Sebelum Penambahan Kolom Input.....	43
Gambar 4.38	Komponen Connection Setelah Penambahan Kolom Input.....	43
Gambar 4.39	Topologi Pengujian Secure Websocket.....	44
Gambar 4.40	Tangkapan Packet Proses Autentikasi.....	45
Gambar 4.41	Payload Packet Proses Autentikasi.....	45
Gambar 4.42	Penggabungan Password dan Suffix.....	46
Gambar 4.43	Proses Perbandingan Hash Password dan MAC.....	47
Gambar 4.44	Daftar Password Rockyou.....	47
Gambar 4.45	Hasil Cracking Script Python.....	47

Gambar 4.46	Tangkapan Packet Pengiriman Goal.....	48
Gambar 4.47	Payload Packet Pengiriman Goal.....	48
Gambar 4.48	Keadaan Robot Sebelum Pengiriman Goal Dari Attacker.....	49
Gambar 4.49	Perintah Pengiriman Goal Dengan Websocat.....	49
Gambar 4.50	Robot Menerima Goal Dari Attacker.....	50
Gambar 4.51	Robot Bergerak Ke Destinasi Goal.....	50
Gambar 4.52	Robot Sampai Ke Destinasi Goal.....	51
Gambar 4.53	Tangkapan Packet Yang Terenkripsi.....	52
Gambar 4.54	Topologi Pengujian Client Authentication.....	53
Gambar 4.55	Aplikasi Sistem Kontrol di Komputer Client.....	54
Gambar 4.56	Aplikasi Sistem Kontrol di Komputer Attacker.....	54
Gambar 4.57	Tampilan Log ROS di Komputer Host.....	55
Gambar 4.58	Log Proses Autentikasi Yang Gagal di Aplikasi.....	55
Gambar 4.59	Log Proses Autentikasi Yang Gagal di ROS.....	56

DAFTAR LAMPIRAN

Lampiran 1. Kode Lengkap File Launch.....	61
Lampiran 2. Kode Program Fungsi Connect.....	63
Lampiran 2. Kode Program Python Untuk Mengungkap Kata Kunci.....	64



INTISARI

Robotic Operating System (ROS) adalah salah satu framework robot yang populer saat ini. ROS 1 adalah versi ROS yang lama dan masih aktif digunakan dan dikembangkan sampai saat ini. Selain menyediakan fasilitas untuk pengembangan sistem robot, ROS 1 juga menyediakan fasilitas untuk mengembangkan aplikasi sistem kontrol untuk menavigasi, memonitor, dan mengatur perilaku robot.

Banyak artikel dan literatur telah membahas mengenai cara pengembangan aplikasi sistem kontrol untuk robot yang berbasis ROS 1. Akan tetapi, aplikasi sistem kontrol yang dikembangkan tersebut tidak memiliki aspek keamanan. Penulis mengamati bahwa aplikasi tersebut memiliki dua celah yang fatal yaitu komunikasi yang tidak terenkripsi dan tidak adanya proses autentikasi. Melalui penelitian ini, penulis mencoba menerapkan mekanisme pengamanan untuk menutup kedua celah tersebut melalui implementasi Secure WebSocket dan Client Authentication.

Hasil penelitian menunjukkan bahwa implementasi dari Secure WebSocket dan Client Authentication masing-masing dapat mengamankan komunikasi robot dan aplikasi sistem kontrol dari ancaman serangan yang disebabkan oleh kedua celah keamanan tersebut.

Kata kunci: ros, robot, keamanan, websocket, autentikasi

ABSTRACT

Robotic Operating System (ROS) is one of the most popular robot frameworks today. ROS 1 is an older version of ROS and is still being actively used and developed today. In addition to providing facilities for the development of robotic systems, ROS 1 also provides facilities for developing control system applications to navigate, monitor, and regulate robot behavior.

Many articles and literature have discussed how to develop control system applications for robots based on ROS 1. However, the developed control system application does not have a security implementation. The author observes that the application has two fatal security vulnerabilities, namely unencrypted communication and the absence of an authentication process. Through this research, the author tries to implement a security mechanism to close the two vulnerabilities through the implementation of Secure WebSocket and Client Authentication.

The results show that the implementation of Secure WebSocket and Client Authentication can each secure robotic communications and control system applications from the threat of attacks caused by the two aforementioned security vulnerabilities.

Keyword: ros, robot, security, websocket, authentication