

**IMPLEMENTASI PROTOKOL WEBSOCKET PADA SISTEM
KEAMANAN *SAFEBOX* MENGGUNAKAN KODE OTP
(*ONE-TIME PASSWORD*)**

**IGNATIA TRI WENEWASTI
H1051201009**

SKRIPSI



**PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2024**

**IMPLEMENTASI PROTOKOL WEBSOCKET PADA SISTEM
KEAMANAN *SAFEBOX* MENGGUNAKAN KODE OTP
(*ONE-TIME PASSWORD*)**

**IGNATIA TRI WENEWASTI
H1051201009**

Skripsi

Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer



**PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2024**

LEMBAR PENGESAHAN

Judul Tugas Akhir : Implementasi Protokol WebSocket Pada Sistem Keamanan *Safebox* Menggunakan Kode OTP (*One-Time Password*)
Nama Mahasiswa : Ignatia Tri Wenewasti
NIM : H1051201009
Jurusan/Program Studi : Rekayasa Sistem Komputer
Tanggal Lulus : 16 Desember 2024
SK Pembimbing : No.2282/UN22.8/TD.06/2024/Tanggal 7 Agustus 2024
SK Penguji : No.4247/ UN22.8/TD.06/2024/Tanggal 17 Desember 2024

Dosen Pembimbing

Pembimbing I



Ikhwan Ruslianto, S.Kom., M.Cs.
NIP. 198607012014041001

Pembimbing II



Hafiz Muhardi, S.T., M.Kom.
NIP. 199007232023211017

Dosen Penguji

Ketua Penguji



Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 198003192015042001

Anggota Penguji



Kasliono, S.Mat., M.Cs.
NIP. 199306202022031005

Pimpinan Sidang
(merangkap anggota penguji)



Ikhwan Ruslianto, S.Kom., M.Cs.
NIP. 198607012014041001

Sekretaris Sidang
(merangkap anggota penguji)



Hafiz Muhardi, S.T., M.Kom.
NIP. 199007232023211017

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura



Prof. Dr. Gusrizal, S.Si, M.Si
NIP. 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama : Ignatia Tri Wenewasti

NIM : H1051201009

Program Studi/Jurusan : Rekayasa Sistem Komputer

Fakultas : Matematika dan Ilmu Pengetahuan Alam

dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyataan ini untuk digunakan sebagaimana mestinya.

Pontianak, 16 Desember 2024



Ignatia Tri Wenewasti
H1051201009

Implementasi Protokol Websocket Pada Sistem Keamanan *Safebox* Menggunakan Kode OTP (*One-Time Password*)

Abstrak

Sistem keamanan *safebox* umumnya menggunakan *password* atau PIN untuk sistem keamanan pada kotak penyimpanan, namun metode tersebut memiliki kelemahan seperti potensi lupa *password* dan pencurian data PIN. Penelitian ini mengembangkan sistem keamanan *safebox* dengan menggunakan kode OTP (*One-Time Password*) dan protokol WebSocket untuk meningkatkan kecepatan dan stabilitas autentikasi. Sistem ini menggunakan mikrokontroler NodeMCU ESP32, *solenoid door lock*, *keypad*, dan LCD untuk mendukung kinerja operasional perangkat dan Aplikasi Android untuk memudahkan pengguna memonitoring *safebox*. Pengujian dilakukan sebanyak 30 kali untuk mengukur parameter *delay* dan *throughput*. Hasil pengujian menunjukkan bahwa penggunaan protokol WebSocket pada sistem keamanan *safebox* dapat memberikan autentikasi yang lebih cepat, terutama dalam menangani respons secara *real-time* dengan rata-rata *delay* sebesar 71 ms dan rata-rata *throughput* sebesar 258 bps. Berdasarkan standar TIPHON, sistem ini termasuk dalam kategori sangat baik karena rata-rata *delay* berada di bawah ambang batas 150 ms dan *throughput* berada di atas batas minimal 100 bps. Selain itu, keamanan sistem ditingkatkan dengan penerapan kode OTP yang hanya berlaku selama 5 menit serta kemampuan mendeteksi dan menolak *input* kode OTP yang salah, kedaluwarsa, atau tidak sesuai format.

Kata Kunci: *Safebox*, WebSocket, *One-Time Password*, Sistem Keamanan, *Real-Time*.

Implementation of WebSocket Protocol in Safebox Security System Using OTP Code (One-Time Password)

Abstract

Safebox security systems generally use passwords or PINs for security systems in storage boxes, but these methods have weaknesses such as the potential to forget passwords and PIN data theft. This research develops a safebox security system using OTP (One-Time Password) code and WebSocket protocol to increase the speed and stability of authentication. This system uses NodeMCU ESP32 microcontroller, solenoid door lock, keypad, and LCD to support the operational performance of the device and Android application to facilitate users to monitor the safebox. Tests were conducted 30 times to measure delay and throughput parameters. The test results show that the use of the WebSocket protocol in the safebox security system can provide faster authentication, especially in handling real-time responses with an average delay of 71 ms and an average throughput of 258 bps. Based on TIPHON standards, this system is categorized as excellent because the average delay is below the 150 ms threshold and the throughput is above the minimum limit of 100 bps. In addition, the security of the system is enhanced by the implementation of an OTP code that is only valid for 5 minutes as well as the ability to detect and reject input of incorrect, expired, or out-of-form OTP codes.

Keywords: *Safebox, WebSocket, One-Time Password, Security System, Real-Time.*

PRAKATA

Puji syukur atas kehadiran Tuhan Yang Maha Esa yang telah melimpahkan berkat dan karunia-Nya kepada penulis sehingga dapat menyelesaikan tugas akhir yang berjudul “**Implementasi Protokol WebSocket Pada Sistem Keamanan Safebox Menggunakan Kode OTP (*One-Time Password*)**” sebagai syarat untuk mendapatkan gelar Sarjana Komputer (S.Kom.) pada Jurusan Rekayasa Sistem Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura Pontianak.

Semua hasil yang diperoleh ini tidak terlepas dari segala dukungan dan bantuan dari berbagai pihak yang tidak pernah berhenti mendorong agar dapat menyelesaikan tugas akhir ini dengan baik. Sebagai penghargaan, izinkanlah saya mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Kedua Orang Tua yang selalu memberikan dukungan, doa, semangat, dan motivasi tanpa henti sepanjang perjalanan penulisan tugas akhir ini.
2. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
3. Bapak Tedy Rismawan, S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
4. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., sebagai dosen Pembimbing Akademik (PA) sekaligus Dosen Pembimbing Pertama yang telah memberi masukan, motivasi, petunjuk bimbingan, dan pengarahan selama masa perkuliahan dan penyusunan skripsi ini.
5. Bapak Hafiz Muhandi, S.T., M.Kom., sebagai Dosen Pembimbing Kedua yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
6. Ibu Dwi Marisa Midyanti, S.T., M.Cs., sebagai dosen Penguji Pertama, yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
7. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen Penguji Kedua, yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
8. Yoshafat Andika Pratama sebagai pasangan yang senantiasa mendengarkan keluh kesah peneliti, memberi dukungan, motivasi, pengingat, dan menemani peneliti sehingga skripsi ini dapat diselesaikan dengan baik.

9. Saudari Yohana Esterina yang senantiasa menemani, memberi semangat, dukungan dan bantuan dalam bentuk apapun sehingga penulis dapat menyelesaikan skripsi ini.
10. Saudara Muhammad Raihan yang senantiasa menemani, memberi semangat, dukungan dan bantuan dalam bentuk apapun sehingga penulis dapat menyelesaikan skripsi ini.
11. Rekan-rekan seperjuangan Mahasiswa/i SyComAs 2020 yang telah memberikan semangat dan dukungan dalam proses perkuliahan.
12. Semua pihak yang membantu baik secara langsung maupun tidak langsung dalam membantu penulis menyelesaikan skripsi ini.

Penulis menyadari masih terdapat kekurangan dalam penulisan tugas akhir ini. Oleh karena itu, diharapkan saran, masukan, dan kritik yang membangun dari pembaca untuk perbaikan di masa mendatang.

Pontianak, 16 Desember 2024

Ignatia Tri Wenewasti

DAFTAR ISI

LEMBAR PENGESAHAN	ii
PERNYATAAN INTEGRITAS AKADEMIK	iii
Abstrak	iv
<i>Abstract</i>	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
DAFTAR KODE PROGRAM	xiv
DAFTAR LAMPIRAN	xv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB 2 LANDASAN TEORI	6
2.1 Penelitian Terdahulu	6
2.2 Protokol WebSocket	7
2.3 Protokol HTTP (<i>Hypertext Transfer Protokol</i>)	8
2.4 Pusher	8
2.5 OTP (<i>One-Time Password</i>)	9
2.6 NodeMCU ESP32	10
2.7 Arduino IDE	10
2.8 <i>Solenoid Door Lock</i>	11
2.9 <i>Keypad</i>	12
2.10 LCD (<i>Liquid Crystal Display</i>) 1602	12
2.11 Flutter	13
2.12 Server	14
2.13 MySQL	14
2.14 <i>Quality of Service (QoS)</i>	15
2.15 <i>Wireshark</i>	16
BAB 3 METODE PENELITIAN	17
3.1 Studi Literatur	18
3.2 Analisis Kebutuhan	18
3.2.1 Kebutuhan Perangkat Keras	18
3.2.2 Kebutuhan Perangkat Lunak	18
3.3 Perancangan Sistem	19
3.3.1 Perancangan Perangkat Keras	19
3.3.2 Perancangan Perangkat Lunak	19
3.4 Implementasi Sistem	19
3.5 Pengujian Sistem	20
3.6 Kesimpulan dan Saran	20
BAB 4 PERANCANGAN	21
4.1 Deskripsi Sistem	21
4.2 Perancangan Arsitektur Sistem	22

4.2.1	<i>Flowchart</i> Sistem.....	23
4.3	Perancangan Perangkat Keras	24
4.3.1	Perancangan Sistem Verifikasi Kode OTP Pada Perangkat Keras	25
4.3.2	Perancangan Sistem Kendali Tombol Pada <i>Safebox</i>	25
4.3.3	Perancangan Keseluruhan Perangkat Keras	28
4.4	Perancangan Perangkat Lunak	28
4.4.1	Perancangan Sistem Komunikasi Protokol Websocket dan HTTP	29
4.4.2	Perancangan Pembuatan Kode OTP (<i>One-Time Password</i>)	31
4.5	Perancangan Basis Data	32
4.5.1	Tabel Data	33
4.6	Perancangan Antarmuka.....	35
4.6.1	Perancangan Antarmuka Aplikasi Android.....	35
4.6.2	Perancangan Halaman Register	36
4.6.3	Perancangan Halaman Beranda	37
4.6.4	Perancangan Halaman Histori Akses <i>Safebox</i>	38
4.7	Perancangan Pengujian	39
4.7.1	Perancangan Pengujian Fungsional	39
4.7.2	Perancangan Pengujian Keamanan.....	39
4.7.3	Perancangan Pengujian Antarmuka Pengguna	39
4.7.4	Perancangan Pengujian Kinerja (QoS) Menggunakan Kode OTP	39
4.8	Perancangan Pengujian <i>Black Box</i>	39
BAB 5	IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN	41
5.1	Implementasi Sistem	41
5.1.1	Implementasi Sistem Keamanan <i>Safebox</i>	41
5.1.2	Implementasi Sistem Kendali Tombol Sistem Keamanan <i>Safebox</i>	42
5.1.3	Implementasi Keseluruhan Perangkat Keras	43
5.1.4	Implementasi <i>Database</i> Sistem Keamanan <i>Safebox</i>	44
5.2	Kode Program	45
5.2.1	Kode Program Pusher	45
5.2.2	Kode Program <i>Header</i>	46
5.2.3	Kode Program <i>Setup</i>	46
5.2.4	Kode Program Mengambil Data Status <i>Safebox</i>	47
5.2.5	Kode Program Mengambil Kode OTP Terbaru	48
5.2.6	Kode Program Kirim Kode OTP	49
5.2.7	Kode Program <i>Loop</i>	50
5.2.8	Kode Program <i>Multitasking Loop</i>	51
5.2.9	Kode Program Membuat Kode OTP	52
5.2.10	Kode Program Verifikasi Kode OTP	53
5.3	Visualisasi aplikasi	54
5.3.1	Halaman Register.....	54

5.3.2 Halaman <i>Login</i>	55
5.3.3 Halaman Beranda.....	55
5.3.4 Halaman Histori Akses <i>Safebox</i>	56
5.4 Pengujian Sistem.....	57
5.4.1 Pengujian Fungsional.....	57
5.4.2 Pengujian Keamanan	59
5.4.3 Pengujian Antarmuka Pengguna.....	60
5.4.4 Pengujian <i>Delay</i> Menggunakan Kode OTP.....	61
5.4.5 Pengujian <i>Throughput</i> Menggunakan Kode OTP.....	64
5.4.6 Pengujian <i>Black Box</i>	67
5.5 Pembahasan.....	68
BAB 6 PENUTUP.....	71
6.1. Kesimpulan.....	71
6.2. Saran.....	71
DAFTAR PUSTAKA	72
LAMPIRAN	75

DAFTAR GAMBAR

Gambar 2. 1 WebSocket <i>Connection</i>	7
Gambar 2. 2 NodeMCU ESP32	10
Gambar 2. 3 Arduino IDE	11
Gambar 2. 4 Solenoid Door Lock	11
Gambar 2. 5 Keypad	12
Gambar 2. 6 LCD 1602	12
Gambar 2. 7 Flutter	13
Gambar 2. 8 Cara kerja server	14
Gambar 3. 1 Diagram Alir Penelitian	17
Gambar 4. 1 Gambaran Sistem Secara Umum	21
Gambar 4. 2 Arsitektur Sistem	22
Gambar 4. 3 Flowchart Sistem	23
Gambar 4. 4 Perancangan Koneksi Pin NodeMCU ESP32 dan LCD1602	26
Gambar 4. 5 Perancangan Koneksi Pin NodeMCU ESP32 dan Relay	26
Gambar 4. 6 Perancangan Pin NodeMCU ESP32 dan Keypad	27
Gambar 4. 7 Perancangan Kunci Safebox	27
Gambar 4. 8 Perancangan Keseluruhan Perangkat Keras	28
Gambar 4. 9 Diagram Alir Perangkat Lunak	29
Gambar 4. 10 Perancangan Menggunakan Protokol Websocket (Pusher)	30
Gambar 4. 11 Perancangan Menggunakan Protokol HTTP	30
Gambar 4. 12 Perancangan Pembuatan kode OTP (<i>One-Time Password</i>)	31
Gambar 4. 13 Relasi Antara Tabel	32
Gambar 4. 14 Flowchart Aplikasi	35
Gambar 4. 15 Tampilan Register Aplikasi Android	36
Gambar 4. 16 Tampilan Login Aplikasi Android	37
Gambar 4. 17 Tampilan Halaman Beranda Aplikasi Android	37
Gambar 4. 18 Tampilan Halaman Histori Akses Safebox	38
Gambar 5. 1 Implementasi Sistem Keamanan Safebox	41
Gambar 5. 2 Implementasi Sistem Kendali Tombol Sistem Keamanan Safebox	42
Gambar 5. 3 Implementasi Keseluruhan Perangkat Keras	43
Gambar 5. 4 Tabel Database User	44
Gambar 5. 5 Tabel Database Otp_log	44
Gambar 5. 6 Tabel Database Otp	45
Gambar 5. 7 Tabel Database Safe_boxes	45
Gambar 5. 8 Tampilan Implementasi Halaman Register	55
Gambar 5. 9 Tampilan Implementasi Halaman Login	55
Gambar 5. 10 Tampilan Implementasi Halaman Beranda	56
Gambar 5. 11 Tampilan Implementasi Halaman Histori Akses Safebox	57
Gambar 5. 12 Pengujian Penggunaan Kode OTP	57
Gambar 5. 13 Pengujian Status OTP invalid (kode OTP yang salah atau acak)	59
Gambar 5. 14 Pengujian Status OTP Time Out	60
Gambar 5. 15 Pengujian Input Kode OTP kurang dari 6 digit angka	60
Gambar 5. 16 (a) Pengujian Fitur Login, (b) Pengujian Request OTP, (c) Pengujian Notifikasi Invalid	60

Gambar 5. 17 Hasil <i>Capture Delay</i> OTP Menggunakan <i>Wireshark</i>	62
Gambar 5. 18 Grafik Pengujian <i>Delay</i> OTP	63
Gambar 5. 19 Hasil <i>Capture Throughput</i> Menggunakan <i>Wireshark</i>	65
Gambar 5. 20 Grafik Pengujian <i>Throughput</i>	66

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	6
Tabel 2. 2 Kategori <i>Throughput</i>	15
Tabel 2. 3 Kategori <i>Delay</i>	16
Tabel 4. 1 Koneksi Pin NodeMCU ESP32 dan LCD1602	26
Tabel 4. 2 Koneksi Pin NodeMCU ESP32 dan <i>Relay</i>	26
Tabel 4. 3 Koneksi Pin NodeMCU ESP32 dan <i>Keypad</i>	27
Tabel 4. 4 Koneksi Pin <i>Solenoid Door Lock</i> dan <i>Relay</i>	27
Tabel 4. 5 Koneksi Pin DC <i>Input</i> dan <i>Relay</i>	27
Tabel 4. 6 Koneksi Pin DC <i>Input</i> dan <i>Solenoid Door Lock</i>	27
Tabel 4. 7 Tabel <i>User</i>	33
Tabel 4. 8 Tabel <i>Otp_log</i>	34
Tabel 4. 9 Tabel <i>Otp</i>	34
Tabel 4. 10 Tabel <i>Safe_boxes</i>	34
Tabel 4. 11 Perancangan Pengujian <i>Black Box</i>	40
Tabel 5. 1 Pengujian Penggunaan Kode OTP.....	58
Tabel 5. 2 Pengujian Status OTP invalid	59
Tabel 5. 3 Tabel Pengujian <i>Delay</i> OTP	61
Tabel 5. 4 Tabel Pengujian <i>Throughput</i>	64
Tabel 5. 5 Pengujian <i>Black Box</i>	67

DAFTAR KODE PROGRAM

Kode Program 5. 1	Kode Program <i>Pusher</i>	46
Kode Program 5. 2	Kode Program <i>Header</i>	46
Kode Program 5. 3	Kode Program <i>Setup</i>	47
Kode Program 5. 4	Kode program Mengambil Data Status <i>Safebox</i>	47
Kode Program 5. 5	Kode Program Mengambil Kode OTP Terbaru	48
Kode Program 5. 6	Kode Program Kirim Kode OTP	49
Kode Program 5. 7	Kode Program <i>Loop</i>	50
Kode Program 5. 8	Kode Program <i>Multitasking Loop</i>	51
Kode Program 5. 9	Kode Program Membuat Kode OTP	52
Kode Program 5. 10	Kode Program Verifikasi Kode OTP	53

DAFTAR LAMPIRAN

Lampiran 1	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-1	75
Lampiran 2	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-2.....	75
Lampiran 3	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-3	75
Lampiran 4	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-4.....	75
Lampiran 5	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-5	76
Lampiran 6	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-6.....	76
Lampiran 7	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-7	76
Lampiran 8	Statistics Pengujian <i>Delay</i> dan <i>Throughput</i> Kode OTP Ke-8.....	76

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Safebox merupakan suatu kotak atau perangkat yang kerap digunakan untuk menyimpan benda-benda berharga (Suyitno & Satriawan, 2021). Kotak penyimpanan umumnya dapat disimpan dimana saja, seperti di rumah, di sekolah, di kantor dan area lainnya. Kotak penyimpanan secara khusus difungsikan dalam melindungi barang berharga dari aksi kriminal seperti perampokan dan pencurian (Wisjhnuadji dkk., 2022). Meskipun sistem keamanan saat ini sudah ada yang menggunakan *password*/pin, sistem keamanan tersebut masih memiliki kelemahan seperti lupa *password*/pin, pencurian data *password*/pin, dan tidak adanya sistem monitoring saat status terkunci atau tidak terkunci (Muhaimin dkk., 2022).

Salah satu metode untuk meningkatkan sistem keamanan dan privasi pengguna adalah dengan menggunakan kode *One-Time Password* (OTP). OTP merupakan sebuah kode yang hanya dapat digunakan untuk satu kali transaksi atau satu sesi. Setelah digunakan sekali, kode OTP tidak dapat dipakai lagi (Giovaniz dkk., 2024). Dalam konteks sistem keamanan *safebox*, penggunaan kode OTP memiliki potensi dalam meningkatkan sistem keamanan karena setiap kali pengguna akan mengakses *safebox*, diperlukan kode unik untuk sistem autentikasi.

Sistem keamanan dengan menggunakan kode OTP akan melakukan komunikasi secara *real-time* antara perangkat dan aplikasi. Namun, sistem keamanan ini menghadapi tantangan terutama saat kecepatan pengiriman dan penerimaan data yang terhubung pada kotak penyimpanan. Pada penelitian yang dilakukan oleh (Afif dkk., 2021) pengujian menggunakan metode OTP menunjukkan hasil *delay* antara 5 hingga 10 detik dengan tingkat keberhasilan 95%. Menurut penelitian yang dilakukan oleh (K. A. Nugraha, 2024), protokol WebSocket adalah pilihan terbaik untuk membangun sistem secara *real-time* karena mampu menghasilkan *latency* rendah sehingga waktu jeda (*delay*) mendekati nol. Pada penelitian (Merdekawan & Sari, 2022) menunjukkan hasil pengujian menggunakan protokol WebSocket dapat menghasilkan *delay* rata-rata sebesar 0.028 detik yang masuk pada kategori bagus.

Penelitian terkait sebelumnya yang pernah dilakukan berjudul “Perbandingan Server Sent Event & Websocket untuk Integrasi Website & Module RFID” (Irawan & Suartana, 2024). Penelitian ini bertujuan untuk membandingkan kecepatan pengiriman dan penerimaan data, serta penggunaan memori dan *bandwidth* dari kedua protokol dalam menentukan protokol yang lebih efektif dalam sistem *self-checkout*. Hasil dari penelitian menunjukkan protokol Websocket lebih unggul daripada protokol Server Sent Event (SSE) dengan *delay* waktu 3.5 - 4.2 *miliseconds* dan protokol SSE 4.1 - 5.2 *miliseconds*. Dalam penelitian ini protokol komunikasi untuk integrasi antara RFID dengan aplikasi berbasis website, Websocket lebih unggul dalam *Delay* dan beberapa aspek lain dibandingkan dengan Server Sent Event.

Penelitian lain berjudul “Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses *Push Notification*” (Putra dkk., 2024). Penelitian ini bertujuan untuk menganalisis komparasi antara kedua protokol dalam memahami karakteristik, efisiensi, dan responsivitas masing-masing. Salah satu aspek yang diukur adalah kecepatan pengiriman pesan, yang melibatkan waktu *delay* dan waktu respons dari kedua protokol. Hasil penelitian menunjukkan bahwa protokol WebSocket lebih efektif saat mengatasi *push notification* dalam skenario aplikasi *real-time*, pengujian menunjukkan bahwa rata-rata total *delay* keseluruhan dari *client* uji pada protokol Websocket adalah 0.700 detik, sedangkan pada protokol MQTT adalah 1.008 detik.

Penelitian selanjutnya berjudul “Perancangan Sistem Keamanan Aplikasi Pada Lemari Brankas Dengan Menggunakan Metode OTP” (Afif dkk., 2021). Berdasarkan hasil pengujian yang telah dilakukan, sistem keamanan brankas pada penelitian ini dapat bekerja secara optimal dengan tingkat keberhasilan 95%. Aplikasi Android yang digunakan dapat mempermudah pengguna untuk mengakses kode OTP yang telah dikirim. Metode OTP (*One Time Password*) yang digunakan pada penelitian cocok untuk digunakan pada lemari brankas, sehingga dapat menambah sistem keamanan yang ada.

Berdasarkan latar belakang yang telah diuraikan, diperlukan pengembangan sistem yang dapat meningkatkan komunikasi secara *real-time* antara perangkat dan aplikasi pada sistem keamanan *safebox*. Untuk mengatasi hal tersebut maka dilakukan penelitian dengan judul “Implementasi Protokol WebSocket Pada Sistem

Keamanan *Safebox* Menggunakan Kode OTP (*One-Time Password*)". Teknologi ini diterapkan untuk meningkatkan sistem keamanan dan kecepatan autentifikasi menggunakan kode OTP pada sistem keamanan *safebox*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat rumusan masalah sebagai berikut:

1. Bagaimana penggunaan protokol WebSocket terhadap *delay* pada proses pengiriman OTP dalam sistem keamanan *safebox*?
2. Bagaimana penggunaan protokol WebSocket terhadap *throughput* pada proses pengiriman OTP dalam sistem keamanan *safebox*?

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian ini sebagai berikut:

1. Objek yang digunakan pada satu buah *safebox* (kotak penyimpanan).
2. Menggunakan Mikrokontroler NodeMCU ESP32 DOIT V1.
3. *Solenoid Door Lock* 12V DC untuk mengunci *safebox*.
4. LCD1602 untuk menampilkan informasi OTP.
5. *Keypad* 4×4 matrix (*hard keypad*) untuk *input* OTP.
6. Aplikasi yang dibuat berbasis Android.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain sebagai berikut:

1. Mengetahui penggunaan protokol WebSocket terhadap *delay* pada proses pengiriman OTP dalam sistem keamanan *safebox*.
2. Mengetahui penggunaan protokol WebSocket terhadap *throughput* pada proses pengiriman OTP dalam sistem keamanan *safebox*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk meningkatkan keamanan dengan penggunaan kode OTP dan implementasi protokol WebSocket untuk komunikasi secara *real-time* dalam penggunaan *safebox* sehingga dapat mempercepat proses autentifikasi. Sistem ini juga dilengkapi dengan aplikasi Android yang

memungkinkan pengguna dapat menerima notifikasi secara *real-time* ketika ada aktivitas akses yang pada *safebox* sehingga dapat meminimalkan risiko pencurian.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi 6 bab agar permasalahan dapat dijelaskan dan diuraikan untuk menyelesaikan penelitian ini. Adapun sistematika penulisan tugas akhir ini terdiri dari:

BAB 1 PENDAHULUAN

Bab pendahuluan berisi latar belakang untuk menjelaskan kenapa penelitian ini dilakukan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat, penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab landasan teori berisi bahasan mengenai dasar teori pendukung yang digunakan dalam penelitian. Adapun landasan teori pada bab ini diantaranya adalah dasar teori protokol Websocket, protokol HTTP, Pusher, *One-Time Password*, NodeMCU ESP32, Arduino IDE, *Solenoid Door Lock*, *Keypad*, LCD (*Liquid Crystal Display*) 1602, Flutter, Server, MySQL, *Quality of Service* (QoS), dan *Wireshark*.

BAB 3 METODOLOGI PENELITIAN

Bab metode penelitian adalah prosedur atau uraian rencana penelitian yang dilakukan untuk mengumpulkan dan menganalisis data serta menjawab pertanyaan atau hipotesis yang telah ditetapkan dalam penelitian. Adapun isi dari metode penelitian yaitu diagram alir, yang mencakup langkah-langkah studi literatur, pengumpulan data, analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian sistem, kesimpulan dan saran.

BAB 4 PERANCANGAN SISTEM

Bab perancangan sistem menjelaskan tentang rancangan sistem yang dibangun dalam penelitian meliputi penjelasan tentang deskripsi sistem, perancangan arsitektur sistem, perancangan perangkat keras, perancangan perangkat lunak, perancangan pembuatan OTP (*One-Time Password*), perancangan basis data, perancangan antarmuka berbasis Android, dan perancangan pengujian.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan berisi tahapan-tahapan yang dilakukan untuk mengimplementasikan, menguji dan membahas sistem. Tahapan ini yaitu implementasi perangkat keras, implementasi perangkat lunak, pengujian, dan pembahasan yang terdiri dari implementasi sistem, kode program, pengujian sistem dan hasil sistem. Setelah dilakukan pengujian maka dilakukan pembahasan dari hasil pengujian keseluruhan sistem.

BAB 6 PENUTUP

Bab penutup merupakan bab yang membahas tentang kesimpulan dari penelitian yang telah dilakukan dan saran terhadap masalah yang belum terselesaikan untuk dapat diperbaiki dan dikembangkan pada penelitian berikutnya.