PETROGAS: Journal of Energy and Technology

Vol. 6, No. 1, Maret 2024, pp. 21-32 **e-ISSN - 2656-5080**

PEMROGRAMAN SISTEM KEAMANAN WEB ADMINISTRATOR BERDASARKAN IP PUBLIK BERBASIS IOT *(INTERNET OF THINGS)*

Nurjanah[1*], Hamsir[1], Muhammad Ibnu Zein[1], Fitri Oktafiani[1]

Program Studi Teknik Instrumentasi Elektronika Migas,
Sekolah Tinggi Teknologi Migas, Balikpapan
*E-mail: surga.bunyu@gmail.com

ABSTRACT

This research offers an innovative solution for implementing an IoT (Internet of Things) based web administrator security system. This research uses a wiring design that has been realized, the system can monitor and control access to the administrator dashboard based on the public IP address of the accessor. Using Lolin (WeMos) D1 R1 as a microcontroller and I2C LCD for data display, users can easily manage web access efficiently. Through the Arduino IDE application using the C/C++ programming language, this system can be set up with setup and loop functions, ensuring proper initialization and repeated processing of access requests. The test results of this system successfully demonstrated its ability to detect unauthorized access and block it with a fast response. An unknown IP will be detected on the system and turn on the alarm/buzzer and the public IP will appear on the LCD. This system also sends notifications via the Telegram application, providing greater convenience and control for users. In its development, this system can be applied and combined with various devices as a control and security system.

Keywords*: Web Administrator, Internet of Things, Public IP, Lolin (WeMos) D1 R1, Arduino IDE*

ABSTRAK

Penelitian ini menawarkan solusi inovatif dalam menerapkan sistem keamanan web administrator berbasis IoT *(Internet of Things)*. Penelitian ini menggunakan desain wiring yang telah direalisasikan, sistem dapat memonitor dan mengontrol akses ke dashboard administrator berdasarkan alamat IP publik pengakses. Penggunaan Lolin (WeMos) D1 R1 sebagai mikrokontroler dan LCD I2C untuk tampilan data, pengguna dapat dengan mudah mengelola akses web secara efisien. Melalui aplikasi Arduino IDE dengan menggunakan bahasa pemrograman C/C++, sistem ini dapat diatur dengan fungsi setup dan loop, memastikan inisialisasi yang tepat dan pemrosesan permintaan pengakses secara berulang. Hasil pengujian sistem ini berhasil menunjukkan kemampuannya dalam mendeteksi akses tidak sah dan memblokirnya dengan respons yang cepat. IP yang tidak dikenali akan terdeteksi pada sistem dan menyalakan alarm/*buzzer* dan I public akan muncul di LCD. Sistem ini juga mengirimkan notifikasi melalui aplikasi telegram, memberikan kenyamanan dan kontrol yang lebih baik bagi pengguna. Dalam perkembangannya, sistem ini dapat diaplikasikan dan digabungkan dengan berbagai *device* sebagai sistem kontrol dan keamanan.

Kata kunci: *Web Administrator*, Internet of Thing, IP Publik, *Lolin (WeMos) D1 R1*, *Arduino IDE*

Artikel diterima 26 Februari 2024. Online 30 Maret 2024.

PENDAHULUAN

Peretasan pada sistem informasi menjadi hal yang paling sering terjadi dalam lingkup Informasi Teknologi berupa kebocoran data (*data leak*) milik pengguna, kerusakan sistem seperti defacing, sistem down akibat serangan DoS atau DDoS, akses masuk tidak sah (*unauthorized access*) pada web administrator, dan masih banyak lagi kejadian peretasan yang terjadi pada sistem informasi publik (Alneyadi, et al., 2016; Engebretson, 2013; Singh & Silakari, 2009).

Peretasan yang sangat marak terjadi, pemerintah Indonesia menerbitkan beberapa Undang-Undang terkait aksi peretasan yang dilakukan pada sistem informasi. Peretasan adalah suatu pelanggaran hukum. Aturan terkait peretasan telah dimuat dalam Undang-Undang (UU) 11/2008 tentang Informasi dan Transaksi Elektronik ITE). Adapun salah satu Undang-Undang yang menjadi acuan yang melatar belakangi dibuatnya judul Tugas Akhir ini adalah pada Pasal 30 ayat 3 UU No 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".

Kasus peretasan yang terjadi pada sebuah sistem biasanya diketahui setelah terjadinya serangan. Sebagai contoh dalam kasus kebocoran data (*data leaked*) dapat diketahui setelah adanya laporan dari seseorang bahwa data pada sistem mereka terpublikasi. Pada kasus lain seperti *defacing* diketahui ketika halaman web diakses dan tampilan berubah tidak sebagaimana mestinya. Semua insiden siber tersebut diketahui oleh pemilik sistem setelah kejadian peretasan dilakukan (Atzori, et al., 2010; Rahardjo, 2005; Setiawan & Setiyadi, 2018).

Penerapan IoT *(Internet of Thing)* memungkinkan pemilik sistem dapat memonitor dan mengontrol akses tidak sah ke dashboard web administrator sebagai lokasi aktivitas user mengelola data (Rose & Chapin, 2015). Sistem Keamanan Web Administrator dapat digunakan pada suatu perusahaan, kantor, dan organisasi sebagai sistem kontrol dan keamanan untuk menghindari terjadinya kebocoran data dan gangguan dari akses yang tidak sah. Atas dasar keamanan data ini penulis melakukan penelitian mengenai Pemrograman Sistem Keamanan Web Administrator Berdasarkan IP Publik Berbasis IoT dengan menggunakan mikrokontroler Arduino IDE dan Telegram. Penggunaan Telegram telah banyak dimanfaatkan salah satunya sebagai media informasi penelitian (Mulyanto, 2020)

METODE PENELITIAN

Penelitian ini dilakukan dari bulan Juni– Juli 2023. Penelitian ini diawali dengan melakukan studi literatur, merancang alat, membuat alat, dan pengujian alat.

Komponen-Komponen Sistem Keamanan Web

Beberapa komponen yang digunakan dalam penerapan sistem keamanan web administrator sebagai berikut :

A. Lolin (WeMos) D1 R1

Lolin D1 R1, juga dikenal sebagai WeMos D1 R1 adalah salah satu jenis papan pengembangan berbasis mikrokontroler yang populer dalam komunitas IoT dan *prototyping*. Papan ini didasarkan pada mikrokontroler ESP8266 yang merupakan salah satu mikrokontroler Wi-Fi yang paling banyak digunakan untuk proyek IoT. ESP8266 memiliki prosesor berkecepatan tinggi, memori yang cukup untuk kode dan data, serta kemampuan terintegrasi untuk terhubung ke jaringan Wi-Fi. Wemos D1 R1 seperti Gambar 1.

Gambar 1. *Lolin (WeMos) D1 R1*

B. Software Arduino IDE

Arduino IDE adalah *software* yang digunakan untuk membuat *sketch* pemrogaman atau dengan kata lain arduino IDE sebagai media untuk pemrogaman pada *board* yang ingin diprogram. Arduino IDE ini berguna untuk mengedit, membuat, meng-*upload* ke *board* yang ditentukan, dan meng-*coding* program tertentu. Arduino IDE dibuat dari bahasa pemrogaman JAVA, yang dilengkapi dengan *library* C/C++*(wiring)*, yang membuat operasi *input/output* lebih mudah (Hakiki, et al., 2020).

Aplikasi Arduino IDE sebagai bahan untuk menulis, verify dan compile, unggah program, dan memonitor kinerja WeMos. Adapun fitur-fitur yang terdapat dalam Arduino IDE dapat dilihat pada Gambar 2.

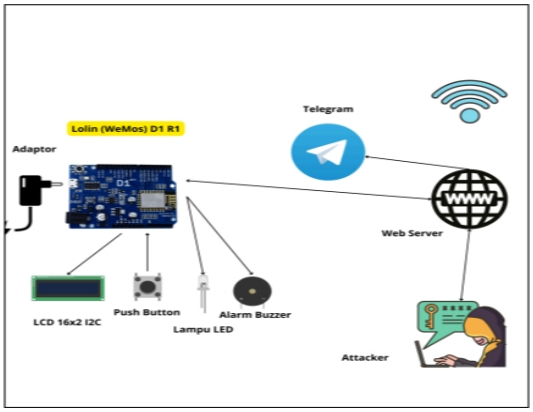
Gambar 2. Arduino IDE

C. Aplikasi XAMPP

XAMPP adalah perangkat lunak sumber terbuka (open-source) yang berfungsi sebagai paket pengembangan web yang lengkap dan siap pakai. Nama "XAMPP" sendiri merupakan singkatan dari X (untuk berbagai sistem operasi), Apache (server web), MySQL (database), PHP (bahasa pemrograman server-side), dan Perl (bahasa pemrograman). Perangkat lunak ini memungkinkan pengguna dengan mudah mengatur lingkungan pengembangan web di komputer lokal, sehingga dapat mengembangkan dan menguji aplikasi web secara lokal sebelum mempublikasikannya ke server online. Aplikasi XAMPP ini sebagai bahan untuk menjalankan program web pada localhost atau local server (Kumari and Nandal, 2017).

Pengujian Alat Sistem Keamanan WEB

Design Sistem Keamanan *Web Administrator* Berdasarkan IP Publik Berbasis IoT dapat dilihat pada Gambar 3. Gambar ini menunjukkan bagaimana alat ini bekerja untuk memonitor dan mengontrol akses milik pengakses berdasarkan alamat IP Publik milik pengakses.



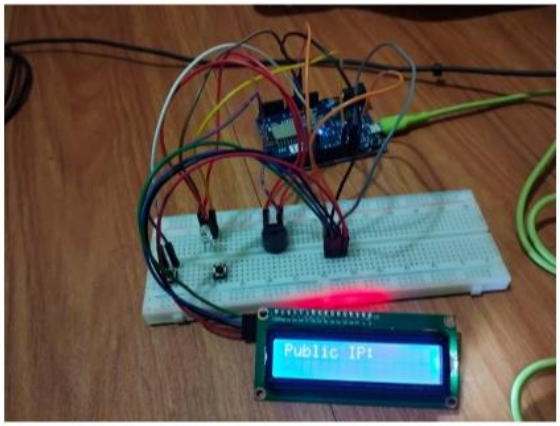
Gambar 3. Sistem Keamanan Web

Adapun langkah-langkah dalam pengujian alat sebagai berikut

1. Alat dinyalakan menggunakan adaptor sebagai pemberi arus listrik pada Lolin (WeMos) D1 R1 dan terhubung ke internet melalui jaringan WiFi;
2. Setelah alat menyala dan terhubung ke internet, alat akan mendapatkan IP Publik milik pengakses jika ada yang mengakses halaman dashboard pada web administrator;
3. Jika IP pengakses didapatkan maka alat akan memberikan peringatan atau notifikasi berupa lampu LED dan alarm buzzer yang menyala dan akan menampilkan IP Publik milik pengakses yang ditampilkan melalui LCD I2C. Web server juga akan mengirimkan IP address pengakses ke aplikasi telegram jika alamat IP tersebut adalah IP yang baru pertama kali mengakses;
4. Jika alamat IP akan diblokir, maka tombol tactical dapat digunakan untuk memblokir IP Publik milik pengakses tidak sah. Sebaliknya, jika IP memiliki akses berizin maka akan dikembalikan ke tahap sebelumnya untuk menerima IP pengakses selanjutnya;

HASIL PENELITIAN DAN PEMBAHASAN

Pada penelitian ini telah dirancang dan direalisasikan seperti Gambar 4. Hasil realisasi ini merupakan bentuk fisik dari alat yang diterapkan untuk sistem keamanan web administrator berdasarkan IP Publik berbasis IoT**.**



Gambar 4. Wiring Sistem Keamanan Web Administrator

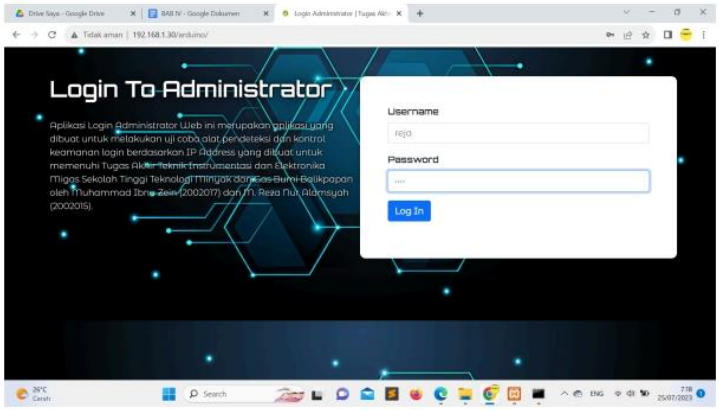
Pada Gambar 4. terdapat komponen berupa *Lolin (WeMos) D1 R1* sebagai mikrokontroler untuk mengolah data yang didapatkan, papan breadboard sebagai papan untuk mengalirkan listrik

keseluruh bagian komponen kerja alat, lampu LED dan alarm buzzer sebagai indikator peringatan atau notifikasi ketika ada pengakses yang mengakses halaman dashboard web administrator, dan tombol tactical (push button) digunakan untuk mengontrol akses IP Publik yang masuk ke dashboard web administrator untuk memblokir akses. Layar LCD berfungsi untuk menampilkan IP Publik.

A. Sistem Kerja Keamanan Web Administrator

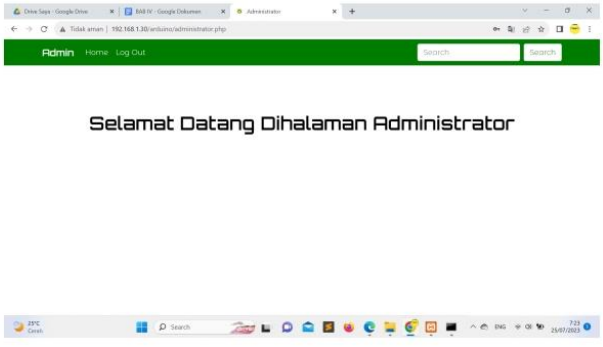
Adapun sistem kerja keamanan Web Administrator bagi pengakses tidak sah sebagai berikut:

a. Melakukan simulasi akses tidak sah ke dashboard administrator dengan melakukan login pada halaman login;



Gambar 5. Halaman Login

b. Pengakses tidak sah berhasil masuk ke halaman dashboard web administrator



Gambar 6. *Dashboard Web Administrator*

c. Alat menangkap IP Publik yang dimiliki oleh pengakses tidak sah dengan menyalakan lampu LED dan alarm buzzer sebagai respon alat dan menampilkan IP Publik pengakses ke layar

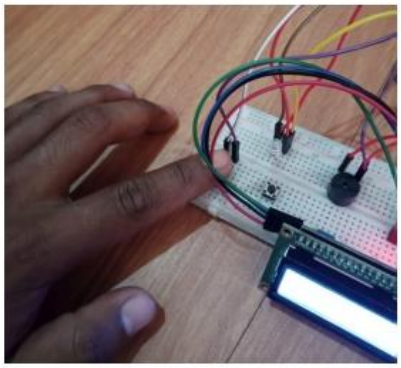
LCD I2C;

Gambar 7. Respon Alat

d. Halaman *dashboard* yang diakses juga akan mengirimkan IP Publik pengakses dan link untuk kontrol akses dashboard administrator ke aplikasi telegram sebagai aplikasi untuk memantau IP baru yang terdaftar;

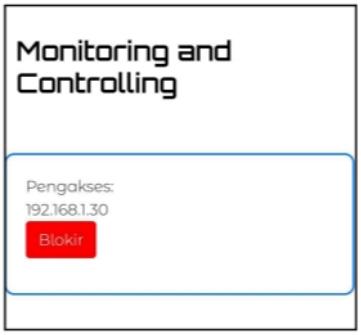
Gambar 8. Aplikasi Telegram Memantau IP Publik

Kontrol akses dapat dilakukan melalui alat dengan menekan tombol tactical (*push button*) sebanyak satu kali untuk memblokir akses pada pengakses tidak sah;



Gambar 9. Blokir Akses Melalui Alat

e. Kontrol akses dapat dilakukan melalui aplikasi telegram dengan membuka link yang dikirimkan oleh bot telegram dan tekan tombol blokir untuk memblokir akses ke telegram. Jika tombol blokir pada link sudah ditekan, maka akan menampilkan pesan "Status berhasil diupdate". Pengakses tidak sah akan dialihkan ke halaman utama Google Search;



Gambar 10. Kontrol Akses Memblokir Pengakses Tidak Sah

Hasil pengujian sistem berhasil menunjukkan kemampuannya dalam mendeteksi akses tidak sah dan memblokirnya dengan respons yang cepat. Sistem ini juga mengirimkan notifikasi melalui aplikasi telegram, memberikan kenyamanan dan kontrol yang lebih baik bagi pengguna.

B. Pemrograman Keamanan Web Administrator

Pembuatan program pada aplikasi arduino IDE sangat dibutuhkan agar *Lolin (WeMos) D1 R1* befungsi dengan baik. Tanpa dimasukan program ke Lolin (WeMos) D1 R1 tidak dapat digunakan untuk menerima dan mengirim data ke web server. Bahasa pemrograman yang digunakan pada arduino IDE ini adalah basis pemrograman C/C++. Adapun penulisan program ini mencakup indikator pendeteksi menggunakan lampu LED dan alarm buzzer, monitor menggunakan LCD I2C, dan pengontrol akses menggunakan tombol tactical. Berikut sistem pemrograman keamanan Web Administrator:

Tahap Awal Program

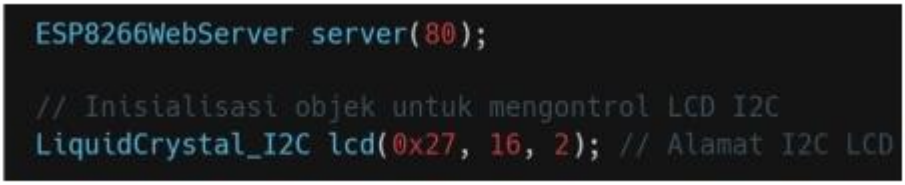
Tahap awal pada pembuatan program pada Arduino IDE untuk Lolin (WeMos) D1 R1 adalah dengan memasukan library yang dibutuhkan dan tahap deklarasi dan inisialisasi pada setiap tipe data untuk menjalankan sintaks dan fungsi tertentu agar dapat mempersingkat dalam penulisan program.

```
#include <ESP8266WiFi.h>
#include <ESP8266WebServer.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

const char* ssid = "kostazri";
const char* password = "yuliati12";

const int ledPin = D5;
const int buttonPin = D6;
bool ledStatus = false;
bool ledRequested = false;
unsigned long ledStartTime = 0;
const long ledDuration = 5000; // Durasi LED menyala (5 detik)

ESP8266WebServer server(80);
```

Gambar 11. Tahap Awal Program

Penggunaan Port Web Server dan Inisialisasi Objek LCD I2C

Lolin (WeMos) D1 R1 pada Penerapan sistem keamanan ini akan membuat web server sendiri dan web server tersebut akan berjalan pada port 80. Port 80 adalah port default yang dimiliki oleh Lolin (WeMos) yang biasanya digunakan sebagai interaksi secara IoT (Internet of Things) entah Lolin (WeMos) pada posisi *client* maupun penggunaannya pada posisi server. Inisialisasi objek pada LCD 16x2 I2C digunakan untuk mengontrol LCD dalam menampilkan data yang telah diprogram. Pada proses inisialisasi objek, alamat LCD sangat penting. Alamat LCD I2C yang digunakan pada penelitian ini adalah 0x27 dan 16, 2 merupakan inisialisasi dari LCD 16x2.



```
ESP8266WebServer server(80);

// Inisialisasi objek untuk mengontrol LCD I2C
LiquidCrystal_I2C lcd(0x27, 16, 2); // Alamat I2C LCD
```

Gambar 12. Penggunaan Port dan inisialisasi LCD 16x2 I2C

Fungsi Setup

Fungsi Setup yang digunakan pada program ini akan digunakan sebagai proses inisialisasi tahapan pertama sebelum memasuki tahapan-tahapan fungsi berikutnya. Adapun kegunaan dari

fungsi setup ini adalah sebagai berikut:

a. Mengatur pin pada lampu LED sebagai output atau keluaran ketika WeMos menerima data dari web administrator dan mengatur keadaan pin sebelum menerima data, yaitu dalam keadaan mati atau LOW;
b. Mengatur button pin atau pin yang terhubung dengan tombol tactical atau push button agar dapat mengaktifkan pull-up internal pada pin D6 WeMos;
c. Inisialisasi LCD I2C untuk menampilkan teks pada baris pertama, yaitu “Public IP: ”;
d. Menghubungkan Lolin (WeMos) D1 R1 ke jaringan WiFi berdasarkan SSID dan Password yang telah dimasukan ke variabel pada tahap awal program;
e. Pembuatan inisial path jika web server pada XAMPP mengirim permintaan HTTP GET untuk menyalakan lampu LED dan alarm buzzer pada server.on jika web server sudah diaktifkan;
f. Menampilkan teks “Web Server Telah Aktif” pada serial monitor.

```
void setup() {
  Serial.begin(115200);
  pinMode(ledPin, OUTPUT);
  digitalWrite(ledPin, LOW); // Pastikan LED mati pada awalnya

  pinMode(buttonPin, INPUT_PULLUP); // Mengaktifkan pull-up inter

  // Inisialisasi LCD I2C
  lcd.begin();
  lcd.print("Public IP:"); // Tampilkan pesan "Public IP:" pada b

  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Menghubungkan ke WiFi...");
  }

  Serial.println("Tersambung ke WiFi");
  Serial.println(WiFi.localIP());

  server.on("/", handleRoot);
  server.on("/nyalakan_led", handleLEDOn);
  server.on("/set_public_ip_and_led", handleSetPublicIPAndLED);

  server.begin();
  Serial.println("WebServer telah aktif");
}
```

Gambar 13. Fungsi Setup

Fungsi Loop

Fungsi loop akan dieksekusi secara berulang-ulang setelah fungsi setup. Penggunaan fungsi loop pada program ini adalah untuk menghandle client yang mengirim permintaan ke web server pada WeMos dan akan menyalakan lampu LED dan alarm buzzer selama waktu yang ditentukan yaitu selama 5 detik ketika ada pengakses yang mengakses halaman dashboard web administrator. Deklarasi fungsi checkButtonState dimasukan agar ketika tombol ditekan masih bisa digunakan lagi

ketika ada pengakses dengan IP address terbaru.

```
void loop() {
  server.handleClient();
  checkButtonState();

  if (ledRequested && !ledStatus) {
    // Nyalakan LED dan catat waktu saat ini
    digitalWrite(ledPin, HIGH);
    ledStatus = true;
    ledStartTime = millis();
  }

  if (ledStatus && (millis() - ledStartTime >= ledDuration)) {
    // Matikan LED setelah mencapai durasi yang diinginkan
    digitalWrite(ledPin, LOW);
    ledStatus = false;
    ledRequested = false;
  }
}
```

Gambar 14. Fungsi Loop

Fungsi send DataToServer

Fungsi sendDataToServer dengan nilai (*value*) berupa tipe data String untuk dikirimkan atau melakukan request ke web server pada XAMPP melalui protokol HTTP dengan request method POST.

```
void sendDataToServer(String data) {
  // Alamat IP atau alamat domain dari server PHP Anda
  String serverAddress = "http://192.168.1.30/arduino/kontrol.php"; // Sesuaikan dengan alamat API PHP Anda
  String contentType = "application/x-www-form-urlencoded"; // Change to the appropriate content type if needed

  // Membuat objek WiFiClient untuk koneksi
  WiFiClient client;

  // Menghubungkan ke server
  if (client.connect("192.168.1.30", 80)) {
    // Membuat permintaan POST
    String request = "POST /arduino/kontrol.php HTTP/1.1\r\n";
    request += "Host: 192.168.3.16\r\n";
    request += "Content-Type: " + contentType + "\r\n";
    request += "Content-Length: " + String(data.length()) + "\r\n\r\n";
    request += data + "\r\n";

    // Mengirim permintaan ke server
    client.print(request);

    Serial.println("Request:");
    Serial.println(request);

    // Tunggu hingga server merespons
    while (client.connected() && !client.available()) {
      delay(1); // Wait for data
    }

    // Membaca respon dari server
    String response;
    while (client.available()) {
      char c = client.read();
      response += c;
    }

    Serial.println("Response:");
    Serial.println(response);

    // Menutup koneksi
    client.stop();
  } else {
    Serial.println("Koneksi gagal ke server");
  }
}
```

Gambar 15. Fungsi send DataToServer

KESIMPULAN

Setelah dilakukannya seluruh rangkaian alur penelitian pada Penerapan Sistem Keamanan Web Administrator Berdasarkan IP Publik Berbasis IoT (*Internet of Thing*s) didapatkan yaitu Sistem Keamanan Web Administrator Berdasarkan IP Publik Berbasis IoT diterapkan melalui *embedded system* untuk mempermudah dalam menerima indikasi peringatan yang lebih dini terkait kasus peretasan yang sering terjadi. Pemrograman sistem keamanan web administrator berdasarkan IP Publik Berbasis IoT berjalan dengan baik. IP Publik pengakses terbaru terkirim ke telegram dan ditampilkan ke LCD I2C. Proses kontrol juga berjalan dengan baik untuk memblokir akses penyerang ke dashboard web administrator.

UCAPAN TERIMA KASIH

Terima kasih kepada seluruh tim Teknik Instrumentasi Elektronika Migas atas kerjasamanya dan kampus STT Migas Balikpapan yang telah memfasilitasi terlaksananya penelitian ini.

DAFTAR PUSTAKA

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. Journal of Network and Computer Applications, 62, pp. 137-152.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15), pp. 2787-2805.

Engebretson, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.

Hakiki, M. I., Darusalam, U., & Nathasia, N. D. (2020). Konfigurasi Arduino IDE Untuk Monitoring Pendeteksi Suhu dan Kelembapan Pada Ruang Data Center Menggunakan Sensor DHT11. Jurnal Media Informatika Budidarma, 4(1), pp. 150-156.

Kumari, P., and Nandal, R. 2017. A Research Paper OnWebsite Development Optimization Using Xampp/PHP. *International Journal of Advanced Research in Computer Science*, 8(5), p.1231.

Mulyanto, A. D. (2020). Pemanfaatan Bot Telegram Untuk Media Informasi Penelitian. *MATICS: Jurnal Ilmu Komputer dan Teknologi Informasi (Journal of Computer Science and Information Technology)*, 12(1), pp. 49-54.

Rahardjo, B. (2005). *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Indonesia, Bandung.

Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. *The internet Society (ISOC)*, 80, pp. 1-50.

Setiawan, E. B, and Setiyadi, A. (2018). Web Vulnerability Analysis and Implementation. *IOP Conference Series: Materials Science and Engineering*, 407(1), p.012081.

Singh, S., & Silakari, S. (2009). A Survey of Cyber Attack Detection Systems. *International Journal of Computer Science and Network Security*, 9(5), pp. 1-10.