Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 5434 – 5444 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

ANALISIS KEAMANAN LALU LINTAS WEB PADA PERANGKAT IOT ESP8266 MENGGUNAKAN TEKNIK SNIFFING PAKET

Sofyan Pariyasto[1], Raja Tama Andri Agus[2], Fitria Priyulida[3], Rina Julita[4]
[1]Informatika Medis, Sekolah Tinggi Ilmu Kesehatan Mitra Sejati, Medan
[2]Universitas Royal, Kisaran
[3]Universitas Sari Mutiara Indonesia, Medan
[4]Universitas Dehasen, Bengkulu
e-mail: [1]spariyasto@gmail.com, [2]rajatama2588@gmail.com, [3]fpriyulida27@gmail.com, [4]rinajj72@gmail.com

Abstract: *Technological developments in recent years have increased quite rapidly, especially in the field of IoT (Internet of Things). With the increasing development of IoT, of course, in line with the increasing use of IoT devices in everyday life. With the increasing number of IoT devices, the issue of data security in IoT devices is certainly one of the important things that must be considered. In this study, a security analysis of web data traffic was conducted on the IoT NodeMCU esp8266 device. The experiment was conducted using two IoT devices acting as senders and receivers of data and one computer device as an attacker. In the analysis process, three scenarios were carried out: sending data without encryption, sending data with base64 encryption without a key, and finally sending data with XOR encryption with a key inserted in the header of the sent data packet. The tapping process was carried out using Wireshark software. From the results of the trials carried out, the entire data transfer process between the two IoT devices can be fully intercepted by Wireshark. Plaintext data (without encoding) tends to be easier to obtain information, while data with encryption without a key on base64 must be analyzed for its pattern to be able to be decrypted. And for encryption that requires a key in XOR, further analysis is carried out by looking for the key inserted in the header so that decryption can be carried out.*

Keywords: *Internet Of Things (IOT); Wireshark; NodeMCU; Base64 Encoding, XOR Encoding.*

Abstrak: Perkembangan teknologi dalam beberapa tahun terakhir meningkat dengan cukup pesat khususnya dalam bidang IOT (Internet Of Things). Dengan semakin meningkatnya perkembangan IOT tentu sejalan dengan meningkatnya penggunaan perangkat IOT dikehidupan sehari-hari. Dengan semakin banyaknya perangkat IOT yang ada tentu masalah keamanan data dalam perangkat IOT menjadi salah satu hal penting yang harus diperhatikan. Dalam penelitian ini dilakukan analisa keamanan lalu lintas data web pada perangkat IOT NodeMCU esp8266. Percobaan dilakukan dengan menggunakan 2 perangkt IOT yang bertindak sebagai pengirim dan penerima data dan satu perangkat komputer sebagai penyerang. Dalam proses analisa dilakukan tiga skenario yaitu pengiriman data tanpa enkripsi, pengiriman data dengan enkripsi base64 tanpa key, dan yang terakhir pengirimn data dengan enkripsi XOR dengan key disisipkan di header paket data yang dikirim. Proses penyadapan dilakukan dengan menggunakan perangkat lunak Wireshark. Dari hasil ujicoba yang dilakukan seluruh proses transfer data antara kedua perangkat IOT dapat disadap sepenuhnya oleh Wireshark. Data plaintext (tanpa encoding) cenderung lebih mudah didapatkan informasinya, sementara data dengan enkripsi tanpa key pada base64 harus dianalisa polanya untuk bisa dilakukan dekripsi. Dan untuk enkripsi yang membutuhkan key pada XOR dilakukan analisa lanjutan dengan mencari key yang disisipkan diheader agar bisa lakukan dekripsi.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 5434 – 5444 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Kata kunci: Internet Of Things (IOT); Wireshark; NodeMCU; Base64 Encoding, XOR Encoding.

PENDAHULUAN

Dalam beberapa tahun terakhir perkembangan teknologi menujukan peningkatan yang sangat pesat, khusus dalam bidang IOT (Internet of Things). Peningkatan yang cukup pesat tersebut tentunya juga membawa dampak bagi kehidupan. Dampak yang cukup terasa dalam pengguaan IOT (Internet of Things) bisa kita jumpai pada bidang Industri, bidang pertanian, bidang kesehatan bahkan hingga bidang pendidikan. Dengan adanya IOT memungkinkan berbagai perangkat seperti sensor, aktuator, dan mikrokontroler untuk saling terhubung dan bertukar informasi melalui jaringan internet. Namun di balik kemudahan dan manfaat yang diberikan, masih terdapat tantangan yang cukup serius terutama dalam hal keamanan data.

Salah satu hal yang menyebabkan perangkat IOT cukup rawan dalam masalah keamanan adalah karena banyak perangkat IoT yang masih menggunakan protokol komunikasi terbuka seperti HTTP, dimana seluruh informasi dikirimkan dalam bentuk teks tanpa perlindungan enkripsi. Kondisi tersebut menjadikan komunikasi data rentan terhadap penyadapan dan modifikasi oleh pihak yang tidak bertanggung jawab.

Dalam skala pengembangan kecil, NodeMCU ESP8266 menjadi salah satu perangkat yang banyak dipilih oleh para pengembang karena harganya yang relatif terjangkau serta kemudahan dalam proses pembuatan skema ujicobanya. Meskipun NodeMCU ESP8266 memiliki beberapa kelebihan, perangkat ini memiliki keterbatasan dalam sumber daya, sehingga banyak pengembang tidak menerapkan protokol komunikasi yang lebih aman seperti HTTPS atau TLS.
Akibatnya, berbagai data sensor seperti suhu, kelembapan, ataupun status perangkat dikirim melalui HTTP biasa tanpa perlindungan apa pun. Kondisi ini membuka peluang bagi penyerang untuk melakukan penyadapan jaringan. Dengan hanya berada pada jaringan Wi-Fi yang sama, seseorang dapat menangkap lalu lintas data menggunakan aplikasi seperti Wireshark dan membaca informasi yang dikirim tanpa memerlukan kemampuan teknis yang tinggi.

Berdasarkan permasalahan tersebut, penelitian ini dilakukan untuk mengevaluasi tingkat keamanan komunikasi data IoT yang masih menggunakan HTTP. Penelitian menggunakan dua perangkat NodeMCU ESP8266 yang berfungsi sebagai pengirim dan penerima data, serta satu komputer yang digunakan untuk melakukan penyadapan paket menggunakan aplikasi Wireshark. Proses pengujian dilakukan dalam tiga skenario berbeda, yaitu pengiriman data dalam bentuk plaintext, pengiriman data yang telah dienkode menggunakan Base64, serta pengiriman data yang dimodifikasi menggunakan metode XOR dengan kunci tertentu. Melalui pendekatan ini, peneliti ingin melihat seberapa mudah data dari masing-masing skenario terbaca pada hasil tangkapan paket serta sejauh mana metode penyembunyian sederhana dapat melindungi informasi dari potensi penyadapan.

Penelitian ini mencoba mengevaluasi tingkat keamanan komunikasi IoT yang masih menggunakan HTTP. Dua buah NodeMCU ESP8266 digunakan sebagai pengirim dan penerima data, sementara sebuah komputer bertindak sebagai penyadap. Pengujian dilakukan dengan tiga skenario berbeda: pengiriman data dalam bentuk plaintext, data yang di-encode menggunakan Base64, serta data yang dimodifikasi menggunakan metode XOR dengan kunci tertentu. Melalui pendekatan ini, penelitian ingin menunjukkan bahwa teknik

penyembunyian data yang sederhana belum cukup untuk memberikan perlindungan yang nyata terhadap serangan penyadapan.

Penelitian ini diharapkan dapat memberikan gambaran lebih jelas mengenai risiko keamanan pada sistem IoT yang belum menerapkan protokol terenkripsi. Struktur pembahasan dalam artikel ini adalah sebagai berikut: Bab 2 memuat tinjauan pustaka terkait keamanan IoT dan teknik penyandian data sederhana. Bab 3 menjelaskan metode penelitian dan konfigurasi perangkat yang digunakan. Bab 4 menyajikan hasil pengamatan paket data menggunakan Wireshark pada tiga skenario pengujian. Bab 5 membahas temuan serta implikasinya terhadap keamanan sistem IoT. Terakhir, Bab 6 menyimpulkan hasil penelitian dan memberikan saran teknis mengenai peningkatan keamanan komunikasi data pada perangkat IoT.

Keamanan data pada sistem Internet of Things (IoT) memang jadi perhatian besar, terutama karena semua perangkat di dalamnya saling bertukar informasi yang kadang sifatnya cukup sensitif. Dalam dunia keamanan jaringan, ada tiga prinsip dasar yang selalu jadi acuan hal itu meliputi kerahasiaan, integritas, dan ketersediaan, atau yang lebih dikenal sebagai CIA Triad. Masalah biasanya muncul ketika data tadi bisa disadap pihak lain melalui proses penyadapan dalam jaringan. Selain itu ada juga risiko data diubah selama proses pengiriman oleh pihak ketiga, serta keamanan terkait perangkat yang tiba-tiba sulit diakses karena serangan yang membuat perangkat menjadi terganggu. Tiga komponen ini pada akhirnya menjadi fondasi utama saat merancang sistem komunikasi IoT yang aman.

Protokol HTTP sendiri bekerja sebagai jalur komunikasi antara klien dan server, khususnya dalam lalu lintas data antara kedua perangkat IOT. Data yang dilewatkan pada Protokol HTTP ini tidak dilindungi enkripsi, sehingga isi pesannya benar-benar terlihat apa adanya. Data sensor, kredensial pengguna, sampai informasi lain yang sifatnya pribadi bisa dengan mudah ditangkap menggunakan alat seperti Wireshark atau tcpdump[18]. Untuk menutup celah itu, digunakanlah HTTPS yang membawa enkripsi SSL/TLS agar jalur komunikasinya lebih aman. Namun perangkat IoT, terutama yang berbasis mikrokontroler seperti ESP8266, kadang belum mampu menangani HTTPS karena keterbatasan kapasitas perangkatnya.

Berbagai cara ditempuh untuk menjaga komunikasi IoT tetap aman tanpa harus memakai enkripsi berat seperti TLS yang kadang terlalu membebani perangkat kecil. Di lapangan, sering kali dipilih solusi yang lebih ringan seperti teknik encoding, misalnya Base64 atau XOR. Base64 ini sebenarnya hanya mengubah data biner menjadi teks ASCII supaya lebih mudah dikirim lewat protokol berbasis teks. Jadi sifatnya cuma merapikan data, bukan mengamankan, karena siapa pun bisa mengembalikan hasilnya ke bentuk asli dengan sangat mudah. Sementara XOR sering dipakai sebagai "enkripsi ringan" dengan mencampurkan data dan kunci tertentu sehingga hasilnya tampak acak. Masalahnya, jika kuncinya ketahuan atau mudah ditebak, pola XOR juga cepat terbaca. Karena itu, kedua metode ini lebih pas disebut sebagai teknik penyamaran data, bukan perlindungan data yang benar-benar kuat.

Penelitian soal keamanan komunikasi IoT sendiri sudah banyak dilakukan beberapa menyoroti bagaimana protokol di tingkat aplikasi perlu dibuat lebih aman agar privasi pengguna IoT tetap terjaga. Dapat dilihat bahwa bahwa banyak perangkat IoT masih mengandalkan protokol terbuka seperti HTTP dan MQTT tanpa enkripsi, sehingga mudah sekali disadap. Salah satu solusi kemaanan yang ditawarkan adalah pendekatan berbasis fog computing, dengan ide utama memindahkan proses enkripsi lebih dekat ke perangkat IoT agar data lebih terlindungi. Hanya saja, sebagian besar penelitian tersebut fokus pada sistem

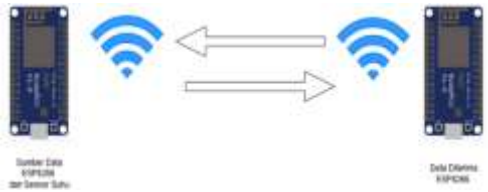
berukuran besar. Penelitian ini mencoba mengisi celah tersebut dengan melihat secara langsung bagaimana data IoT bisa disadap dan dianalisis menggunakan Wireshark pada kondisi nyata dengan perangkat NodeMCU ESP8266.

METODE

Penelitian ini menggunakan pendekatan eksperimental (experimental research approach) untuk mengevaluasi keamanan komunikasi IoT berbasis HTTP. Pendekatan eksperimental dipilih karena memungkinkan peneliti untuk mengontrol lingkungan pengujian, mereplikasi skenario serangan, serta mengukur hasil tangkapan data secara empiris. Dalam konteks keamanan jaringan, metode ini sangat efektif untuk mengamati perilaku paket data saat melintasi jaringan terbuka tanpa enkripsi. Teori dasar yang digunakan mengacu pada konsep network sniffing dan packet inspection, yaitu proses penangkapan dan analisis data yang dikirim melalui jaringan untuk memahami struktur dan isi komunikasinya.

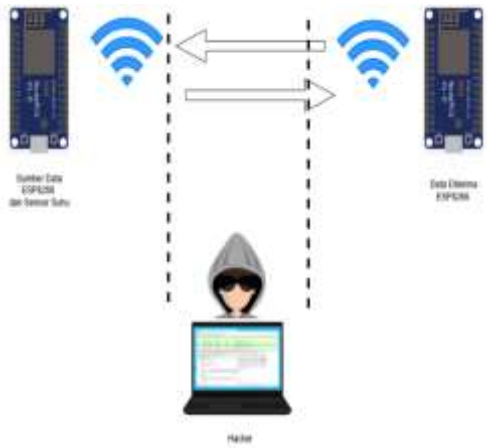
Lingkungan pengujian dibangun dengan menggunakan dua perangkat NodeMCU ESP8266 dan satu komputer yang dilengkapi perangkat lunak Wireshark. NodeMCU pertama berperan sebagai pengirim data (client), sedangkan NodeMCU kedua berperan sebagai penerima sekaligus access point (AP). Perangkat penerima menjalankan web server sederhana menggunakan pustaka ESP8266WebServer yang mendengarkan permintaan HTTP POST dari NodeMCU pengirim. Komputer berfungsi sebagai pihak ketiga (attacker) yang bertugas menangkap seluruh lalu lintas jaringan menggunakan Wireshark. Dengan konfigurasi ini, data dapat dianalisis untuk mengamati bagaimana pesan dikirim, diterima, dan disadap secara langsung pada jaringan lokal.

Prosedur penelitian dimulai dengan menyiapkan kode pada NodeMCU pengirim untuk mengirimkan tiga jenis pesan HTTP POST secara bergantian. Skenario pertama mengirimkan data dalam format plaintext JSON berisi parameter device, temp, dan pesan.



Gambar 1. Skema komunikasi Data antara perangkat IOT

Skenario kedua mengirimkan data JSON yang terlebih dahulu dienkode menggunakan metode Base64 sebelum dikirim. Skenario ketiga menggunakan metode XOR untuk mengenkripsi data JSON menjadi format heksadesimal dan menyertakan kunci rahasia pada header HTTP X-KEY. Pada sisi penerima, NodeMCU kedua menerima permintaan HTTP dan menampilkan data yang diterima melalui halaman web lokal. Sementara itu, komputer dengan Wireshark menangkap seluruh paket jaringan untuk dianalisis lebih lanjut.



Gambar 2. Skema Penyadapan Data dalam jaringan

Data hasil tangkapan Wireshark diekspor dalam format CSV untuk memudahkan analisis dan pengelompokan berdasarkan jenis payload. Setiap paket HTTP diperiksa untuk mengidentifikasi pola keterbacaan, struktur data, serta kemungkinan decoding.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 5434 – 5444 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Gambar 3. Skema target penyadapan data

Evaluasi dilakukan dengan menilai sejauh mana data dapat dipahami oleh pihak ketiga yang tidak memiliki akses ke perangkat pengirim atau penerima. Selain itu, dilakukan analisis terhadap efektivitas Base64 dan XOR dalam menyamarkan isi pesan. Hasil observasi ini digunakan untuk membandingkan antara tiga skenario pengiriman dan menentukan tingkat keamanan masing-masing pendekatan dalam konteks komunikasi IoT yang sederhana dan tidak terenkripsi.

HASIL DAN PEMBAHASAN

Dari hasil proses pengujian yang dilakukan didapatkan hasil berupa log tangkapan data yang telah di eksport dalam format CSV. Data tersebut berisi informasi, waktu, sumber lalu lintas data, tujuan lalu linstas data, protocol yang digunakan, panjang data, serta informasi tambahan.

Tabel 1. Hasil tangkapan log data dengan Wiresharak

No.	Time	Source	Destination	Protocol	Length	Info
36	0.852671	192.168.4.1	192.168.4.3	TCP	227	80 > 53799 [PSH, ACK] Seq=1 Ack=285 Win=1860 Len=173 [TCP PDU reassembled in 37]
37	0.855128	192.168.4.1	192.168.4.3	HTTP/JSON	186	HTTP/1.1 200 OK , JSON (application/json)
38	0.855246	192.168.4.3	192.168.4.1	TCP	54	53799 > 80 [ACK] Seq=285 Ack=307 Win=65230 Len=0
39	0.855882	192.168.4.3	192.168.4.1	TCP	54	53799 > 80 [FIN, ACK] Seq=285 Ack=307 Win=65230 Len=0
40	0.857014	192.168.4.3	192.168.4.1	TCP	66	53805 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
41	0.860081	192.168.4.1	192.168.4.3	TCP	54	80 > 53799 [ACK] Seq=307 Ack=286 Win=1859 Len=0
42	0.860580	192.168.4.1	192.168.4.3	TCP	62	80 > 53805 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536 SACK_PERM
43	0.860660	192.168.4.3	192.168.4.1	TCP	54	53805 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
44	0.860908	192.168.4.3	192.168.4.1	HTTP	338	GET /latest HTTP/1.1
45	0.863100	192.168.4.1	192.168.4.3	TCP	227	80 > 53800 [PSH, ACK] Seq=1 Ack=285 Win=1860 Len=173 [TCP PDU reassembled in 46]

46	0.865082	192.168.4.1	192.168.4.3	HTTP/JSON	186	HTTP/1.1 200 OK , JSON (application/json)
47	0.865221	192.168.4.3	192.168.4.1	TCP	54	53800 > 80 [ACK] Seq=285 Ack=307 Win=65230 Len=0
48	0.865625	192.168.4.3	192.168.4.1	TCP	54	53800 > 80 [FIN, ACK] Seq=285 Ack=307 Win=65230 Len=0
49	0.866312	192.168.4.3	192.168.4.1	TCP	66	53806 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
50	0.870264	192.168.4.1	192.168.4.3	TCP	54	80 > 53800 [ACK] Seq=307 Ack=286 Win=1859 Len=0
51	0.870433	192.168.4.1	192.168.4.3	TCP	62	80 > 53806 [SYN, ACK] Seq=0 Ack=1 Win=2144 Len=0 MSS=536 SACK_PERM
52	0.870512	192.168.4.3	192.168.4.1	TCP	54	53806 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
53	0.870755	192.168.4.3	192.168.4.1	HTTP	338	GET /latest HTTP/1.1
54	0.873210	192.168.4.1	192.168.4.3	TCP	227	80 > 53801 [PSH, ACK] Seq=1 Ack=285 Win=1860 Len=173 [TCP PDU reassembled in 55]
55	0.875637	192.168.4.1	192.168.4.3	HTTP/JSON	186	HTTP/1.1 200 OK , JSON (application/json)
56	0.875741	192.168.4.3	192.168.4.1	TCP	54	53801 > 80 [ACK] Seq=285 Ack=307 Win=65230 Len=0

Dari tabel 1. Terdapat beberapa data yang berisi informasi dalam HTTP/JSON. Data ini nantinya yang akan dianalisa dari sisi body dan headernya. Analisa awal yang dilakukan yaitu menampilkan data dalam bentuk plaintext.

Analisis Skenario Plaintext

Analiss yang dilkukan di tahap awal yaitu analisis data yang dilewatkan secara langsung melalui protocol HTTP. Dalam penelitian ini, skenario pertama menggunakan NodeMCU ESP8266 sebagai pengirim data yang terhubung ke NodeMCU penerima melalui jaringan lokal Wi-Fi yang disediakan oleh perangkat penerima itu sendiri (mode

Access Point). Format data yang kirim merupakan data text/Json tanpa enkripsi yang berisi informasi nama Device perangkat IOT pengirim data, data Temperature serta data pesan tambahan. Data yang bershasil disadap melalui aplikasi Wireshark akan langsung dianalisa pada bagian body untuk diketahui informasi apa yang terkandung dalam plaintext tersebut. Adapun tampilan wireshark dalam proses

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 5434 – 5444 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

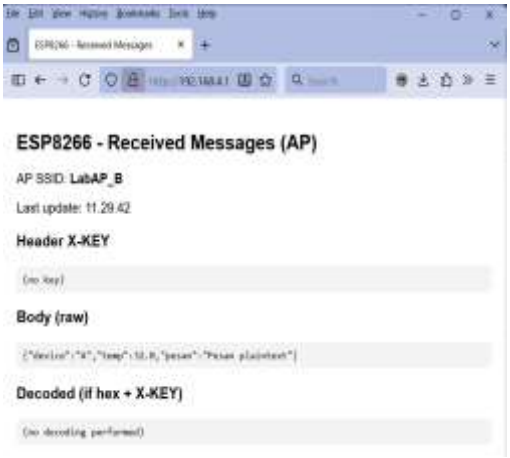
pencarian informasi plaintext terlihat seperti gambar 4 berikut.

Gambar 4. Analisa tanggkapan data Plaintext dengan Wireshark

Dari gambar 4 terlihat bahwa data dikirim dalam bentuk JSON biasa tanpa proses encoding atau enkripsi tambahan. :

{"device":"A","temp":20.3,"pesan":" Pesan plaintext"}

Hasil tangkapan Wireshark menunjukkan bahwa setiap paket POST dari NodeMCU pengirim berisi payload yang dapat dibaca secara utuh dalam tab Packet Details. Field Content-Type ditampilkan sebagai text/plain, dan bagian isi pesan terlihat jelas sebagai JSON lengkap, terlihat seperti gambar 5 berikut.



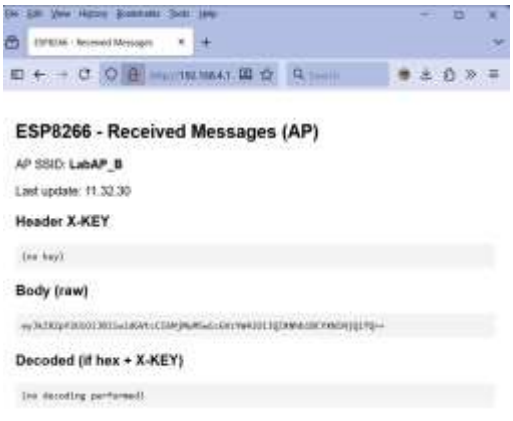
Gambar 5. Tampilan ESP8266 Sebagai AP menampilkan data plaintext

Hal ini menunjukkan bahwa komunikasi HTTP antar NodeMCU berlangsung dalam format terbuka tanpa lapisan enkripsi atau encoding apa pun. Seorang penyerang yang berada di jaringan yang sama dapat dengan mudah mengekstrak data seperti nilai suhu (temp) dan isi pesan (pesan) tanpa perlu alat tambahan selain Wireshark. Fakta ini menegaskan bahwa HTTP dalam bentuk aslinya tidak memberikan perlindungan privasi maupun kerahasiaan data.

Berdasarkan hasil observasi tersebut, dapat disimpulkan bahwa komunikasi IoT berbasis HTTP plaintext tidak aman untuk aplikasi yang memerlukan kerahasiaan data. Meskipun format JSON memberikan struktur yang rapi untuk pertukaran informasi, namun tidak memiliki mekanisme pengamanan terhadap penyadapan atau modifikasi. Pada jaringan publik atau lingkungan industri, penggunaan HTTP tanpa enkripsi berpotensi membuka peluang bagi serangan man-in-the-middle (MITM) yang dapat menyisipkan, mengubah, atau mencuri data. Oleh karena itu, skenario ini membuktikan pentingnya penerapan lapisan keamanan tambahan seperti TLS untuk mengenkripsi komunikasi, bahkan pada perangkat sederhana seperti NodeMCU ESP8266.

Analisis Skenario Base64

Analisis kedua dilakukan dengan cara mengubah data plaintext yang dikirim dengan melakukan encoding dengan Base64 untuk menyembunyikan plaintext. Proses encoding yang dilakukan ditahapan ini tidak menambahkan lapisan keamanan lain, dan hanya mengubah bentuk plaintext menjadi chipertext. Chipertext kemudian dikirim melalui protocol HTTP, terlihat seperti gambar 6 berikut.



Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 5434 – 5444 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Gambar 6. Tampilan ESP8266 Sebagai AP menampilkan data encoding base64

Dalam penelitian ini, NodeMCU ESP8266 yang bertindak sebagai pengirim dikonfigurasi untuk melakukan encoding data JSON ke dalam Base64 sebelum mengirimkannya melalui HTTP POST. Payload awal yang dikirim:

{"device":"A","temp":26.1,"pesan":" Pesan Base64"}

Data yang di encode akan berubah bentuk menjadi string panjang seperti berikut :

eyJkZXZpY2UiOiJBIiwidGVtcCI6MjYuMSwicGVzYW4iOiJQZXNhbiBCYXNlNjQifQ==

Dalam percobaan yang dilakukan menggunakan Wireshark berhasil menangkap seluruh paket HTTP POST dari NodeMCU pengirim. Pada tab Packet Bytes, payload tampak sebagai serangkaian karakter acak yang berakhiran tanda == (perhatikan gambar 7).

Gambar 7. Analisa tanggkapan data Base64 encoding dengan Wireshark

Penggunaan Encoding menggunakan Base64 dapat membantu menyembunyikna informasi yang dikirim mencadi string acak, namun hal ini tidak menambah perlindungan apa pun terhadap proses penyadapan. Hasil pengamatan menunjukkan bahwa penggunaan Base64 tidak memberikan peningkatan keamanan komunikasi IoT secara signifikan. Teknik ini masih memungkinkan penyerang untuk memperoleh dan membaca data asli dengan mudah, karena proses decoding dapat dilakukan tanpa kunci.

Analisis Skenario XOR (Hexadecimal)

Analisa ketiga yang dilakukan yaitu dengan menggunakan metode XOR (exclusive OR). Dalam eksperimen ini, NodeMCU ESP8266 pengirim dikonfigurasi untuk melakukan proses XOR terhadap data JSON sebelum mengirimkannya ke server. Kunci yang digunakan, yaitu "kunciRahasia", diulang secara siklis untuk setiap byte pesan. Setelah proses XOR selesai, hasilnya dikonversi ke bentuk heksadesimal agar dapat dikirim melalui protokol HTTP, terlihat seperti gambar 8 berikut.

Gambar 8. Tampilan ESP8266 Sebagai AP menampilkan data Chiper XOR

Dalam proses ini plaintext yang akan dikirim diencoding terlebih dahulu dan kemudian dikirim melalui body sementara key dikirim melalui header.

NodeMCU penerima dikonfigurasi untuk mendeteksi apakah body pesan berbentuk heksadesimal dan memiliki header X-KEY. Jika ditemukan, data didekripsi kembali dengan operasi XOR menggunakan kunci tersebut, dan hasil akhirnya ditampilkan dalam format JSON yang dapat dibaca, terlihat seperti gambar 9 berikut..

Gambar 9. Analisa tanggkapan data XOR Chiper dengan Wireshark

Hasil tangkapan data mengguankan wiresharek memperlihatkan deretan karakter heksadecial yang terlihat acak. Sementar jika dilihat dibagian header terlihat informasi berupa key dengan value "kunciRahasia" dan dibagian body berisi infomasi string sebagai beriku .

10570A061F3B020D43494B2049594C170C3F114A5B405A4F52594C130C21000643494B310E060F0D490A2E3A491B0C19425713

Hasil deskripsi nya berupa informasi device dan suhu.

{"device":"A","temp":33.9,"pesan":"Pesan XOR(hex)"}

Secara teknis, metode XOR memberikan obfuscation (penyamaran) yang lebih baik dibandingkan Base64 karena hasil enkripsinya tidak langsung terbaca. Namun, karena kunci dikirim bersama paket, skema ini gagal memenuhi prinsip dasar kriptografi, yaitu menjaga kerahasiaan kunci. XOR hanya efektif jika kunci benar-benar rahasia dan digunakan sekali (one-time pad), tetapi dalam eksperimen ini, penggunaan kunci statis menjadikannya mudah diretas.

SIMPULAN

Dari penelitian yang dilakukan dapat di evaluasi tingkat keamanan komunikasi HTTP pada perangkat IoT berbasis NodeMCU ESP8266 menggunakan alat analisis jaringan Wireshark. Dari hasil tiga skenario yang diujicobakan yaitu plaintext, Base64, dan XOR, terlihat bahwa seluruh bentuk komunikasi tanpa enkripsi tetap dapat disadap dan dibaca oleh pihak ketiga. Data yang dikirim melalui HTTP tanpa lapisan keamanan tambahan muncul dapat terlihat secara terbuka melaui hasil tangkapan dengan aplikasi Wireshark, termasuk nilai sensor dan pesan teks yang dikirim antar NodeMCU. Hal ini menunjukkan bahwa penggunaan HTTP murni dalam sistem IoT menimbulkan risiko besar terhadap kerahasiaan dan integritas data, bahkan dalam jaringan lokal sekalipun.

Dari sisi keamanan jaringan, eksperimen ini memperlihatkan betapa mudahnya serangan penyadapan dilakukan pada sistem IoT yang tidak menggunakan enkripsi. Hanya dengan alat sederhana seperti Wireshark, penyerang dapat menganalisis struktur paket, melihat isi pesan, serta mempelajari pola komunikasi antar perangkat. Kondisi ini memperkuat pentingnya kesadaran keamanan bagi pengembang sistem IoT, terutama dalam tahap desain arsitektur komunikasi. Penelitian ini juga memberikan wawasan sederhana bahwa sekadar mengubah bentuk data melalui encoding seperti Base64 atau XOR tidak benar-benar dapat memberikan keamanan data. Proses Encoding yang dilakukan hanya menyembunyikan data secara visual, naum tidak bisa melingdungi data dari akses ilegal pengguna yang tidak sah.

DAFTAR PUSTAKA

G. H. Sandi and Y. Fatma, "PEMANFAATAN TEKNOLOGI INTERNET OF THINGS (IOT) PADA BIDANG PERTANIAN," 2023.

B. Harsanto, "INOVASI INTERNET OF THINGS PADA SEKTOR PERTANIAN: PENDEKATAN ANALISIS SCIENTOMETRICS Internet of Things Innovation in Agriculture Sector: A Scientometrics Analysis."

Anggy Giri Prawiyogi and Aang Solahudin Anwar, "Perkembangan Internet of Things (IoT) pada Sektor Energi : Sistematik Literatur Review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2,

pp. 187–197, Jan. 2023, doi: 10.34306/mentari.v1i2.254.

K. Wójcicki, M. Biegańska, B. Paliwoda, and J. Górna, "Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review," Mar. 01, 2022, *MDPI*. doi: 10.3390/en15051806.

F. Nahdi and H. Dhika, "Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang 33."

Arjun Pratikto Wahyu Hendrawan and Ni Putu Agustini, "Simulasi Kendali Dan Monitoring Daya Listrik Peralatan Rumah Tangga Berbasis ESP32," *ALINIER JURNAL*, 2022.

M. F. Wicaksono and M. D. Rahmatya, "Implementasi Arduino dan ESP32 CAM untuk Smart Home," *Jurnal Teknologi dan Informasi*, doi: 10.34010/jati.v10i1.

Danang Danang, Ekky Fredyan, and Iman Saufik Suasana, "Prototype Alat Keamanan Rumah Internet Of Things (Iot) Berbasis Nodemcu Esp8266 Dengan Esp32 Cam Dan Kombinasi Sensor Menggunakan Telegram," *UNITECH*, 2022.

A. Bhattacharjya, "A HOLISTIC STUDY ON THE USE OF BLOCKCHAIN TECHNOLOGY IN CPS AND IOT ARCHITECTURES MAINTAINING THE CIA TRIAD IN DATA COMMUNICATION," *International Journal of Applied Mathematics and Computer Science*, vol. 32, no. 3, pp. 403–413, Sep. 2022, doi: 10.34768/amcs-2022-0029.

A. Copyright @ Farkhan Nindyarayhan Dhanendra and I. Sujarwo, "Strategi Keamanan pada Sistem Bank Air Kami v2 menggunakan Trias CIA," *Journal Of Social Science Research*, vol. 4, pp. 1048–1062, 2024.

A. H. Harahap, C. Difa Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder".

M. S. Al Reshan, "IoT-based Application of Information Security Triad," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 24, pp. 61–76, 2021, doi: 10.3991/IJIM.V15I24.27333.

K. A. Yousif Yaseen, "Importance of Cybersecurity in The Higher Education Sector 2022," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20–24, Dec. 2022, doi: 10.51983/ajcst-2022.11.2.3448.

H. J. Jara Ochoa, R. Peña, Y. Ledo Mezquita, E. Gonzalez, and S. Camacho-Leon, "Comparative Analysis of Power Consumption between MQTT and HTTP Protocols in an IoT Platform Designed and Implemented for Remote Real-Time Monitoring of Long-Term Cold Chain Transport Operations," *Sensors*, vol. 23, no. 10, May 2023, doi: 10.3390/s23104896.

S. Handaja, K. Dewi, and R. H. Triyanto, "Wireless Volume Corrector for Natural Gas Flow Metering Using ESP32 Microcontroller and Open-Source Web Server." [Online]. Available: www.joiv.org/index.php/joiv

A. Komparatif Konsumsi Daya Baterai pada Perangkat IoT Menggunakan Protokol Komunikasi MQTT dan HTTP and R. Mirza, "Analisis Komparatif Konsumsi Daya Baterai pada Perangkat IoT Menggunakan Protokol Komunikasi MQTT dan HTTP," vol. 02, no. 02, [Online]. Available: https://jurnal.komputasi.org/index.php/jst/article/view/35

W. Khalid, M. Jamil, A. A. Khan, and Q. Awais, "Open-Source Internet of Things-Based Supervisory Control and Data Acquisition System for Photovoltaic Monitoring and Control Using HTTP and TCP/IP Protocols," *Energies (Basel)*, vol. 17, no. 16,

Aug. 2024, doi: 10.3390/en17164083.

K. T. M. Tran, A. X. Pham, N. P. Nguyen, and P. T. Dang, "Analysis and Performance Comparison of IoT Message Transfer Protocols Applying in Real Photovoltaic System," *International Journal of Networked and Distributed Computing*, vol. 12, no. 1, pp. 131–143, Jun. 2024, doi: 10.1007/s44227-024-00021-4.

U. Brawijaya, I. Sentosa, H. Prasetio, and A. Pinandito, "Implementasi Kompresi Data Dengan Menggunakan Zlib Data Compression dan Encoding Base64 Pada Sistem Paratransit Trip Data Collection Berbasis Esp32," 2017. [Online]. Available: http://j-ptiik.ub.ac.id

D. Pradeka, Z. Khaerunnisa, S. Aqila Humaira, and A. Salsa Billa, "Digital Data Security Using a Combination of Base64 Encoding, Rail Fence Cipher, and GZIP Compression Pradeka et al., Digital Data Security Using a Combination of Base64 Encoding, Rail Fence Cipher … |52," *COELITE)*, vol. 4, no. 1, pp. 51–60, 2025, doi: 10.17509/coelite.v4i1.82498.

A. F. Cobantoro, M. B. Setyawan, and H. Oktavianto, "Rekayasa Aplikasi Eposal Menggunakan Algoritma Base64 Untuk Menyimpan Data Pengguna," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 7, no. 1, pp. 31–38, May 2023, doi: 10.31603/komtika.v7i1.8711.

D. Protic and M. Stankovic, "XOR-Based Detector of Different Decisions on Anomalies in the Computer Network Traffic," 2023.

G. Golovko, A. Matiashenko, and N. Solopihin, "DATA ENCRYPTION USING XOR CIPHER," *Системи управління, навігації та зв'язку. Збірник наукових праць*, vol. 1, no. 63, pp. 81–83, Feb. 2021, doi: 10.26906/sunz.2021.1.081.

O. Thinnukool, T. Panityakul, and M. Bano, "Double encryption using trigonometric chaotic map and XOR of an image," *Computers, Materials and Continua*, vol. 69, no. 3, pp. 3033–3046, 2021, doi: 10.32604/cmc.2021.019153.

"Vulnerability Analysis and Password Cracking Using Wireshark." [Online]. Available: https://ieeexplore.ieee.org/document/8014711

N. A. L. Mabsali, H. Jassim, and J. Mani, "Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic," in *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, Atlantis Press International BV, 2023, pp. 114–135. doi: 10.2991/978-94-6463-110-4_10.

T. Wu, F. Breitinger, and S. Niemann, "IoT network traffic analysis: Opportunities and challenges for forensic investigators?," *Forensic Science International: Digital Investigation*, vol. 38, Oct. 2021, doi: 10.1016/j.fsidi.2021.301123.

S. K. Shandilya, C. Ganguli, I. Izonin, and P. A. K. Nagar, "Cyber attack evaluation dataset for deep packet inspection and analysis," *Data Brief*, vol. 46, Feb. 2023, doi: 10.1016/j.dib.2022.108771.

A. Hussain, A. Hussain, S. Qadri, A. Razzaq, H. Nazir, and M. S. Ullah, "Enhancing LAN Security by Mitigating Credential Threats via HTTP Packet Analysis with Wireshark", doi: 10.56979/602/2024.

M. Syaffiq, A. Malek, and A. R. Amran, "A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity," 2021.