# ANALISA KEAMANAN PROTOKOL HTTPS DALAM PENGIRIMAN DATA SUPPLY CHAIN MANAGEMENT SYSTEM PADA JARINGAN WIRELESS DENGAN MENGGUNAKAN METODE MAN IN THE MIDDLE

**SKRIPSI**


**Oleh:**

**MUHAMMAD FATHUR ROHMAN**

**09011181823020**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2025**

# ANALISA KEAMANAN PROTOKOL HTTPS DALAM PENGIRIMAN DATA SUPPLY CHAIN MANAGEMENT SYSTEM PADA JARINGAN WIRELESS DENGAN MENGGUNAKAN METODE MAN IN THE MIDDLE

**SKRIPSI**

**Diajukan Untuk Melengkapi Salah Satu Syarat**

**Memperoleh Gelar Sarjana Komputer**


**Oleh:**

**MUHAMMAD FATHUR ROHMAN**

**09011181823020**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**


**2025**

# HALAMAN PENGESAHAN

# ANALISA KEAMANAN PROTOKOL HTTPS DALAM PENGIRIMAN DATA SUPPLY CHAIN MANAGEMENT SYSTEM PADA JARINGAN WIRELESS DENGAN MENGGUNAKAN METODE MAN IN THE MIDDLE

**SKRIPSI**

**Jurusan Sistem Komputer**

**Jenjang S1**

**Oleh**

**MUHAMMAD FATHUR ROHMAN**

**09011181823020**

**Palembang, 17 Januari 2025**

**Mengetahui,** 21/1/25

| | |
|---|---|
| **Ketua Jurusan Sistem Komputer** | **Pembimbing Tugas Akhir** |
| **Dr. Ir. Sukemi, M.T** | **Ahmad Fali Oklilas, M.T** |
| **NIP. 196612032006041001** | **NIP. 197210151999031001** |

# HALAMAN PERSETUJUAN

**Telah diuji dan lulus pada:**

**Hari : Jum'at**

**Tanggal : 13 Desember 2024**

**Tim Penguji :**

1. **Ketua : Dr. Ir. Sukemi, M.T.**
2. **Penguji : Huda Ubaya, M.T.**
3. **Pembimbing : Ahmad Fali Oklilas, M.T**

**Mengetahui,** 4/1/25

**Ketua Jurusan Sistem Komputer**

**Dr. Ir. Sukemi, M.T**

**NIP. 196612032006041001**

# HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhammad Fathur Rohman

NIM : 09011181823020

Judul : Analisa Keamanan Protokol HTTPS Dalam Pengiriman Data Supply Chain Management System Pada Jaringan Wireless Dengan Menggunakan Metode Man In The Middle

Hasil Pengecekan Software iThenticate/Turnitin: 7%

Menyatakan bahwa laporan skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

**Palembang, 17 Januari 2025**


**Muhammad Fathur Rohman**
**NIM. 09011181823020**

# HALAMAN PERSEMBAHAN

"*Alhamdulillah*"

(**Penulis, Muhammad Fathur Rohman**)

Skripsi ini dipersembahkan untuk :

Kedua Orang Tua

(**Imam Sholihin** dan **Evi Ilmiati**)

Kedua adik saya

(**Muhammad Harish Al-Amin** dan **Hafizhah Mirfaul Jannah**)

Teman Satu Angkatan

(**Sistem Komputer 2018**)

Dan Almamaterku

(**Universitas Sriwijaya**)

"Sirno Dalane Pati, Nur Sifat, Luber Tanpo Kebek"

*(Hilangkan rasa iri dengki, Jadilah orang bermanfaat, Sederhana & Tetap Rendah Hati)*

(**Filosofi Jawa**)

# KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur kehadirat Allah SWT atas karunia beserta rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Skripsi ini yang berjudul **"Analisa Keamanan Protokol HTTPS Dalam Pengiriman Data Supply Chain Management System Pada Jaringan Wireless Dengan Menggunakan Metode Man In The Middle"**.

Dalam laporan skripsi ini penulis menjelaskan mengenai analisa keamanan protokol HTTPS didalam pengiriman data yang terdapat pada *supply chain management system*, Dimana dalam analisa keamanan protokol tersebut nantinya akan dilakukan pengujian keamanan pada protokol yang diterapkan dengan menggunakan metode MITM. Penulis berharap agar tulisan ini dapat bermanfaat bagi orang banyak.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Skripsi ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Skripsi ini dengan baik dan lancar.

2. Kedua orang tua tercinta yang telah membesarkan serta mendidik dengan penuh kasih sayang dan selalu mengajarkan akan semua hal yang baik yang pastinya sangat bermanfaat. Terimakasih untuk segala do'a, motivasi dan dukungannya baik moril, materil maupun spritual selama ini.

3. Bapak Prof. Dr. Erwin, M.Si, selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Bapak Ahmad Fali Oklilas, M.T. selaku Dosen Pembimbing Skripsi yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Skripsi ini.

6. Prof. Dr. Ir. Siti Nurmaini, M.T, selaku Pembimbing Akademik Jurusan Sistem Komputer.

7. Kepada teman seperjuangan (Al-Insyirah, Ilham Fadli dan Rahmat Hidayat) yang telah berjuang bersama di setiap susah dan senang yang ada.

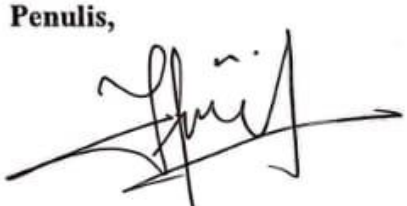
8. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa skripsi ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga Skripsi ini bermanfaat dan berguna bagi khalayak.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

**Palembang, 17 Januari 2025**

**Penulis,**



**Muhammad Fathur Rohman**

**NIM. 09011181823020**

***ANALYSIS OF HTTPS PROTOCOL SECURITY IN DATA DELIVERY SUPPLY CHAIN MANAGEMENT SYSTEMS ON WIRELESS NETWORKS USING MAN IN THE MIDDLE METHOD***

**MUHAMMAD FATHUR ROHMAN (09011181823020)**
*Computer Engineering Department, Faculty of Computer Science*
*Sriwijaya University*
Email: mfr11@gmail.com

# ABSTRACT

*Network security is very important in the increasingly modern era like today, where almost every human activity today requires this, especially the implementation of Warehouse Management Systems which have a lot of sensitive and important data. Therefore, the HTTPS protocol was created as a medium that bridges the process of exchanging information that has good security. However, every security has gaps that make it a weakness, therefore a security test will be carried out on the HTTPS protocol that has been implemented on the system using the Man In The Middle method with several existing techniques, starting from sniffing, ARP Poisoning and also DNS Spoofing. At the end of the research, after carrying out several security tests, starting from the user login process and adding item data, the information sent cannot be seen directly or easily because every data sent has been encrypted. This shows that the HTTPS protocol is able to secure data from security testing experiments that have been carried out.*

***Keywords*** *: HTTPS, Man In The Middle, Sniffing, ARP Poisoning, DNS Spoofing.*

# ANALISA KEAMANAN PROTOKOL HTTPS DALAM PENGIRIMAN DATA SUPPLY CHAIN MANAGEMENT SYSTEM PADA JARINGAN WIRELESS DENGAN MENGGUNAKAN METODE MAN IN THE MIDDLE

**MUHAMMAD FATHUR ROHMAN (09011181823020)**
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: mfr11@gmail.com

## ABSTRAK

Keamanan jaringan merupakan hal yang sangat penting dalam perkembangan zaman yang semakin modern seperti saat ini, dimana hampir setiap kegiatan manusia saat ini semuanya membutuhkan hal tersebut, terutama pengimplementasiannya terhadap sistem manajemen gudang yang memiliki banyak data yang bersifat sensitif dan penting. Maka dari itu diciptakannya protokol HTTPS sebagai media yang menjembatani proses terjadinya pertukaran informasi tersebut yang memiliki keamanan yang baik. Akan tetapi disetiap keamanan memiliki celah yang menjadikannya kelemahan, maka dari itu akan dilakuakan uji keamanan pada protokol HTTPS yang sudah diterapkan pada sistem tersebut dengan menggunakan metode *Man In The Middle* dengan beberapa teknik yang ada, mulai dari sniffing, ARP Poisoning dan juga DNS Spoofing. pada akhir penelitian setelah dilakukan beberapa kali uji keamanan, mulai dari proses login user dan menambahkan data barang, informasi yang dikirimkan tidak dapat dilihat secara langsung atau mudah dikarenakan setiap data yang dikirimkan sudah di enkripsi. Hal ini menunjukkan protokol HTTPS mampu mengamankan data dari percobaan uji keamanan yang telah dilakukan.

**Kata Kunci** : HTTPS, *Man In The Middle*, Sniffing, ARP Poisoning, DNS Spoofing.

# DAFTAR ISI

# DAFTAR GAMBAR

## DAFTAR TABEL

# DAFTAR LAMPIRAN

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Semakin majunya zaman maka hal itu pun diikuti dengan majunya semua ilmu pengetahuan termasuk dengan teknologi, hal tersebut tidak dapat dipungkiri karena dengan adanya semua kemajuan tersebut maka segala sesuatu aktivitas manusia dalam berbagai bidang dapat dibantu serta dipermudah, sehingga pada intinya ilmu pengetahuan serta teknologi tersebut telah memberi sesuatu yang mempunyai banyak manfaat kepada umat manusia.

Salah satu contoh manfaat didalam kemajuan teknologi tesebut adalah dibuatnya suatu sistem berbasis web yang dapat membantu didalam pengelolaan stok barang pada suatu lingkungan pergudangan atau biasa disebut dengan *Supply Chain Management System*, dimana sistem tersebut bertujuan untuk meringankan segala sesuatu yang berhubungan dengan pengelolaan stok barang pada lingkungan pergudangan. Dan juga mengingat pada saat ini pemanfaatan jaringan nirkabel atau *wireless* sangatlah banyak digunakan, sebab dalam pemanfaatannya memiliki banyak kelebihan, diantaranya adalah proses instalasi yang mudah, biaya perawatan yang relative murah, aksesibilitas, dapat digunakan diberbagai perangkat, praktis, fleksibel, nyaman dan juga cepat.

Dalam hal ini, penulis melakukan penelitian serta analisa terhadap sistem yang ada dan sudah disiapkan yang berada pada jaringan nirkabel / WLAN dan menggunakan protokol HTTPS yang sebelumnya masih menggunakan protokol HTTP. Peningkatan keamanan protokol bertujuan guna menghalau terjadinya berbagai serangan yang nantinya akan membahayakan keamanan dari data yang dikirimkan[1].

Pada penelitian ini, penulis mengusulkan akan melakukan uji coba keamanan serta melakukan analisa pada protokol yang digunakan dengan menggunakan metode MITM *(Man In The Middle)* dengan menggunakan menggunakan beberapa jenis pengujian yang berkaitan dengan metode yang diujikan dan nantinya akan memanfaatkan beberapa *tool* guna untuk melakukan analisa terhadap hasil pengujian yang dilakukan[1].

Uji keamanan ini bertujuan untuk mengetahui seberapa efektifkah protokol yang digunakan, apakah keamanan data dapat terjamin pada saat proses pengiriman data yang dilakukan.

## 1.2 Perumusan Masalah

Berdasarkan uraian dari latar belakang yang dijelaskan diatas, maka terdapat suatu hal yang dapat menjadi pokok permasalahan dalam skripsi ini, diantaranya adalah sebagai berikut:

1. Bagaimana cara penerapan uji keamanan pada sistem yang ada dengan menggunakan metode MITM?
2. Seberapa efektifkah protokol HTTPS yang diterapkan pada sistem ketika dilakukan uji keamanan menggunakan metode MITM?

## 1.3 Batasan Masalah

Berdasarkan dari rumusan masalah yang diuraikan, maka berikut di bawah ini yang menjadi batasan masalah pada skripsi ini:

1. Penelitian yang dilakukan akan mengimplemtasikan uji keamanan dengan menggunakan metode MITM dengan beberapa teknik-teknik yang berbeda.
2. Output dari penelitian ini berupa hasil pengujian yang menggunakan metode MITM pada sistem yang sudah diterapkan protokol HTTPS.

## 1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian yang dilakukan antara lain:

1. Menguji keamanan protokol yang digunakan dengan metode MITM dan *tool* yang disiapkan.
2. Untuk mengetahui seberapa efektifkah protokol HTTPS yang diterapkan pada sistem setelah dilakukan pengujian menggunakan metode MITM.

## 1.5 Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan antara lain:

1. Hasil yang diharapkan dapat menjadi salah satu referensi mengenai cara pengujian sistem yang ada dengan menggunakan metode MITM.
2. Hasil yang diharapkan dari penelitian ini dapat menjadi referesni untuk melihat seberapa efektifkah protokol HTTPS yang diterapkan pada sistem setelah dilakukan uji keamanan MITM.

## 1.6 Metodologi Penulisan

Dalam skripsi ini menggunakan metedologi sebagai berikut:

### 1.6.1 Metode Studi Pustaka dan Literatur

Pada bagian metode ini, penulis melakukan pengumpulan dan pencarian referensi atau sumber berupa literatur yang terdapat pada jurnal, paper, buku dan berbagai halaman website mengenai serta yang berhubungan dengan "*Man In The Middle Attack, HTTP/HTTPS Protocol,* Sniffing, ARP Poisoning, DNS Spoofing".

### 1.6.2 Metode Konsultasi

Pada metode ini, Penulis berkonsultasi terlebih dahulu dengan dosen pembimbing dan kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan skripsi "*Man In The Middle attack, HTTP/HTTPS Protocol,* Sniffing, ARP Poisoning, DNS Spoofing".

### 1.6.3 Metode Pengujian

Pada metode ini, melakukan pengujian terhadap sistem yang ada dan juga sudah menerapkan protokol HTTPS dengan menggunakan metode MITM, apakah protokol yang diterapkan tersebut sudah aman dan sesuai apa yang diharapkan.

### 1.6.4 Metode Hasil dan Analisa

Pada metode ini, penulis melakukan analisa pada data yang sudah didapatkan dengan mempertimbangkan beberapa aspek termasuk efektivitas dalam penerapan protokol HTTPS pada sistem yang sudah ada.

### 1.6.5 Metode Penarikan Kesimpulan dan Saran

Pada bagian ini menjadi tahap akhir dari penelitian yang dilakukan. Dimana berdasarkan Hasil dan Analisa, maka penulis akan menarik kesimpulan dan saran tentang masalah dalam penelitian ini, agar dapat menjadi referensi untuk penelitian selanjutnya.

## 1.7 Sistematika Penulisan

Dalam penelitian ini, penulis akan menerapkan susunan penulisan yang terstruktur. Susunan ini digunakan untuk memastikan bahwa penulisan skripsi menjadi lebih rapi dan jelas. Sistem penulisan skripsi yang akan digunakan dalam penelitian ini adalah sebagai berikut:

**BAB I – PENDAHULUAN**

Pada Bab ini akan membahas secara rinci mengenai latar belakang, tujuan, manfaat, perumusan dan batasan masalah, metodologi penelitian, serta sistematika penulisan.

**BAB II – TINJAUAN PUSTAKA**

Pada Bab ini berisikan mengenai dasar teori dan materi yang bersangkutan dengan masalah yang diangkat serta akan diteliti dan konsep dasar yang dibutuhkan untuk menyelesaikan masalah dari penelitian Skripsi ini.

**BAB III – METODOLOGI**

Pada Bab ini akan membahas secara rinci tentang teknik, metode, dan alur proses yang dilakukan dalam penelitian ini.

**BAB IV – HASIL DAN PEMBAHASAN**

Pada Bab ini akan membahas hasil dari pengujian yang telah didapatkan dan menganalisis kekurangan serta kelebihan dari penelitian yang telah dilakukan.

**BAB V – KESIMPULAN DAN SARAN**

Pada bab ini merupakan langkah terakhir dari penelitian, yang akan membahas kesimpulan berdasarkan dari hasil penelitian secara singkat, padat dan jelas, beserta saran untuk penelitian selanjutnya agar mendapatkan hasil dan metode yang lebih baik khususnya tentang penelitian yang telah dikerjakan.

# DAFTAR PUSTAKA

[1] D. Wiharjo and I. R. Widiasari, “Analisis Serangan Man in the Middle (MitM) Menggunakan Firmware Hacking Glinet Router 6416a di Jaringan Wireless Artikel Ilmiah,” no. 672018705, 2019.

[2] G. Tertytchny *et al.*, “Demonstration of Man in the Middle Attack on a Commercial Photovoltaic Inverter Providing Ancillary Services,” *2020 IEEE CyberPELS, CyberPELS 2020*, 2020, doi: 10.1109/CyberPELS49534.2020.9311531.

[3] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, “Man-in-the-Middle Attack Mitigation in Internet of Medical Things,” *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 2053–2062, 2022, doi: 10.1109/TII.2021.3089462.

[4] D. Bruschi, A. Di Pasquale, S. Ghilardi, A. Lanzi, and E. Pagani, “A Formal Verification of ArpON - A Tool for Avoiding Man-in-the-Middle Attacks in Ethernet Networks,” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 6, pp. 4082–4098, 2022, doi: 10.1109/TDSC.2021.3118448.

[5] A. Kosugi, K. Teranishi, and K. Kogiso, “Experimental Validation of the Attack-Detection Capability of Encrypted Control Systems Using Man-in-the-Middle Attacks,” *IEEE Access*, vol. PP, p. 1, 2025, doi: 10.1109/ACCESS.2025.3353289.

[6] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, “Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1638–1653, 2019, doi: 10.1109/TIFS.2018.2883177.

[7] N. Tripathi, M. Swarnkar, and N. Hubballi, “DNS spoofing in local networks made easy,” *11th IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2017*, pp. 1–6, 2018, doi: 10.1109/ANTS.2017.8384122.

[8] A. Jony, M. N. Islam, and I. H. Sarker, “Unveiling DNS Spoofing

Vulnerabilities: An Ethical Examination Within Local Area Networks," in *2023 26th International Conference on Computer and Information Technology, ICCIT 2023*, 2023, pp. 1–6. doi: 10.1109/ICCIT60459.2023.10441649.

[9] T. Pangestu and R. Liza, "Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing," *JiTEKH*, vol. 10, no. 2, pp. 60–67, 2022, doi: 10.35447/jitekh.v10i2.571.

[10] Z. Trabelsi, M. M. A. Parambil, T. Qayyum, and B. Alomar, "Teaching DNS Spoofing Attack Using a Hands-on Cybersecurity Approach Based on Virtual Kali Linux Platform," *IEEE Glob. Eng. Educ. Conf. EDUCON*, pp. 1–8, 2025, doi: 10.1109/EDUCON60312.2025.10578851.

[11] S. A. Samarakoon, "Bypassing Content-based internet packages with an SSL / TLS Tunnel , SNI Spoofing , and DNS spoofing," 2022.

[12] N. V. Limbore *et al.*, "Emerging Trends in Supply Chain Management and its Impact on Business Operations," *Empir. Econ. Lett.*, vol. 22, no. 4, pp. 55–70, 2023, doi: 10.5281/zenodo.8432190.

[13] A. Maraj, E. Rogova, and G. Jakupi, "Testing of network security systems through DoS, SQL injection, reverse TCP and social engineering attacks," *Int. J. Grid Util. Comput.*, vol. 11, no. 1, pp. 115–133, 2020, doi: 10.1504/IJGUC.2020.103976.

[14] A. Bustami and S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review," *Unistek*, vol. 7, no. 2, pp. 59–70, 2020, doi: 10.33592/unistek.v7i2.645.

[15] V. Varadharajan, K. Karmakar, U. Tupakula, and M. Hitchens, "A policy-based security architecture for software-defined networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 897–912, 2019, doi: 10.1109/TIFS.2018.2868220.

[16] A. Mallik, "MAN-IN-THE-MIDDLE-ATTACK : UNDERSTANDING IN SIMPLE," vol. 2, pp. 109–134, 2018.

[17] A. R. Chordiya, “Man-in-the-Middle ( MITM ) Attack Based Hijacking of HTTP Traffic Using Open Source Tools,” *2018 IEEE Int. Conf. Electro/Information Technol.*, pp. 438–443, 2018.

[18] K. Pahlavan and P. Krishnamurthy, “Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective,” *Int. J. Wirel. Inf. Networks*, vol. 28, no. 1, pp. 3–19, 2021, doi: 10.1007/s10776-020-00501-8.

[19] H. Kwon, H. Nam, S. Lee, C. Hahn, and J. Hur, “(In-)Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. 8, pp. 1204–1215, 2020, doi: 10.1109/TIFS.2019.2938416.

[20] I. C. Utomo and S. Rokhmah, “Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta,” *J. Rekayasa Teknol. Inf.*, vol. 6, no. 2, p. 143, 2022, doi: 10.30872/jurti.v6i2.8333.

[21] R. Dastres *et al.*, “Secure Socket Layer ( SSL ) in the Network and Web Security To cite this version :,” 2020.

[22] A. Esfahani *et al.*, “An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4 . 0 Supply Chain,” pp. 1–9, 2019.

[23] S. Royal, “IMPLEMENTASI SSL UNTUK PENCEGAHAN MAN IN THE MIDDLE,” vol. 4307, no. February, pp. 28–33, 2021.

[24] R. Kwon, T. Ashley, J. Castleberry, P. McKenzie, and S. N. Gupta Gourisetti, “Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping,” *2020 Resil. Week, RWS 2020*, no. October, pp. 106–112, 2020, doi: 10.1109/RWS50334.2020.9241271.

[25] H. Berger, A. Z. Dvir, and M. Geva, “A wrinkle in time: a case study in DNS poisoning,” *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 313–329, 2021, doi: 10.1007/s10207-020-00502-x.