Penerapan Teori Otomata dalam Pengujian Keamanan Jaringan untuk Deteksi DdoS

Yusuf Setiawan[1], Benedictus Aurel Deryl Ivan J[2], Gabriel Galih Gumelar[3], Rifian Irionno O[4]

[1]*Teknik Informatika/ Ilmu Komputer*
Jl. Bhayangkara No.55, Tipes, Kec. Serengan, Kota Surakarta
[1]*210103082@mhs.udb.ac.id*

[2]*Teknik Informatika/ Ilmu Komputer*
Jl. Bhayangkara No.55, Tipes, Kec. Serengan, Kota Surakarta
[2]*210103184@mhs.udb.ac.id*

[3]*Teknik Informatika/ Ilmu Komputer*
Jl. Bhayangkara No.55, Tipes, Kec. Serengan, Kota Surakarta
[3]210103055@mhs.udb.ac.id

[4]*Teknik Informatika/Ilmu Komputer*
Jl. Bhayangkara No.55, Tipes, Kec. Serengan, Kota Surakarta
[4]210103075@mhs.udb.ac.id

Abstrak—**Serangan cyber sering kali mengeksploitasi kerentanan dalam sistem jaringan dan perangkat lunak pada sistem untuk mencapai tujuannya khususnya serangan Distributed Denial Of Service (DDOS).Maka pentingya menerapkan Langkah-langkah keamanan yang baik merupakan kunci dalam mencegah serangan cyber.Menerapkan Teori otomata dalam dalam pembuatan sistem ini sangat membantu keamanan yang baik dalam serangan cyber khusnya dalam mendeteksi serangan DDos.Dalam penelitian ini menggunakan Finite State Automata(FSA) untuk deteksi DDos yang terdiri dari sejumlah keadaan (state) dan transisi antara keadaan-keadaan tersebut berdasarkan lalu lintas data yang tidak wajar dalam sebuah sistem.**
Kata kunci— Teori otomata,Keamanan jaringan,Serangan Ddos,Sistem pendeteksi

Abstract—**Cyber attacks often exploit vulnerabilities in network systems and software on systems to achieve their goals, especially Distributed Denial of Service (DDOS) attacks. So the importance of implementing good security measures is key in preventing cyber attacks. Applying Automata Theory in system creation This really helps with good security in cyber attacks, especially in detecting DDoS attacks. In this research, Finite State Automata (FSA) is used for DDoS detection which consists of a number of states and transitions between these states based on abnormal data traffic. in a system.**
Keywords— Automata theory, Network security, Ddos attacks, Detection systems.

I. PENDAHULUAN

A. Latar Belakang

Perkembangan Teknologi Informasi merupakan bukti bahwa manusia terus berpikir ketika menghadapi masalah serta bagaimana mencari solusi untuk memecahkan masalah tersebut, sehingga solusi ini menjadi dasar pembentukan ide-ide baru dalam pengembangan Teknologi Informasi untuk selalu membawa kemudahan dalam kehidupan masyarakat[1]. Sistem Keamanan Jaringan merupakan bentuk dari upaya pencegahan dan pengidentifikasi pengguna jaringan yang tidak sah (penyusup) dari suatu lingkup jaringan. Pencegahan itu dapat menghentikan pengguna yang tidak sah tersebut untuk mengakses setiap hal dalam jaringan yang disusupinya[2]

Distributed Denial of Service (DDoS) adalah ancaman signifikan yang bertujuan membuat layanan atau sumber daya jaringan tidak tersedia bagi pengguna sah dengan cara membanjiri sistem dengan lalu lintas berlebihan. Serangan DDoS sekarang ini menargetkan layanan yang spesifik, sehingga aplikasi yang menjadi target akan menjadi down, sementara komponenjaringan yang lain seperti link, switch, routertidak mengalami masalah[3]. Dengan memanfaatkan teori otomata, pola serangan DDoS dapat dimodelkan untuk mengembangkan alat deteksi yang efektif.

Pengujian alat deteksi ini dilakukan dengan mengimplementasikan model otomata hingga yang mampu mengenali ciri-ciri serangan DDoS, seperti lonjakan lalu lintas dan distribusi IP yang tidak normal. Alat tersebut kemudian diuji pada dataset serangan DDoS untuk mengevaluasi akurasi dan performanya, guna memastikan kemampuannya dalam mengidentifikasi dan mencegah serangan secara real-time.

B. Tinjauan pustaka

a. Teori Bahasa Automata dan Teori Otomata

Teori Bahasa dan Automata merupakan bagian dari ilmu komputer, yang berguna sebagai perantara komunikasi manusia dan mesin. Teori Otomata adalah teori

mengenai mesin-mesin abstrak, dan berkaitan erat dengan teori bahasa formal[4].

b. Keamanan Jaringan dan Serangan DDOS
Keamanan jaringan adalah bidang yang diharapkan dapat ditingkatkan kualitasnya dengan keberadaan teknologi NDN. Dalam hal ini karena keamanan jaringan memerlukan sebuah koordinasi yang baik antara komponen jaringan untuk melakukan pertahanan terhadap serangan. Serangan DDOS sekarang ini menargetkan layanan yang spesifik, sehingga aplikasi yang menjadi target menjadi *down*, sementara komponen jaringan yang lain (*link, switch*, router) tidak mengalami masalah, metode ini membuat serangan bisa menyembunyikan diri sebagai *traffic normal*, karena intensitasnya yang tidak seperti serangan DDOS yang biasanya membuat *traffic* besar-besaran[5].

c. Penerapan Otomata dalam deteksi Anomali Jaringan
Penelitian telah menunjukkan bahwateori otomata dapat diterapkan dalam deteksi anomali jaringan, termasuk serangan DDoS. Automata berhingga dapat digunakan untuk memodelkan dan mengenali pola-pola lalu lintas yang mencurigakan yang menunjukkan bahwa automata berhingga dapat digunakan untuk mendeteksi anomali dalam lalu lintas jaringan dengan memonitor perubahan pola trafik dan mengidentifikasi penyimpangan yang mungkin menunjukkan adanya serangan DDoS[6].

C. Tujuan Penelitian

Tujuan Penulisan penelitian ini adalah:

1. Mempelajari konsep dasar teori otomata dan penerapannya dalam mendeteksi serangan DDoS.
2. Mengembangkan model otomata yang mampu mengidentifikasi pola serangan DdoS.
3. Mengimplementasikan dan menguji alat deteksi DDoS berbasis otomata.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode penelitian dan pengembangan (*Rapid Application Development*) RAD karena menyediakan kerangka kerja yang sistematis dan komprehensif untuk mengembangkan Solusi baru yang didasarkan pada penelitian yang mendalam dan evaluasi yang ketat, pendekatan ini memastikan bahwa alat deteksi yang dikembangkan tidak hanya efektif dan efesien tetapi juga didukung oleh pemahaman ilmiah yang kuat dan terus disempurnakan berdasarkan hasil pengujian dan evaluasi. Adapun tahapan–tahapan yang dilakukan dengan menggunakan metode RAD menurut (Luthfyana, L. F., & Sediyono, E. (2021)) dan terdiri dari beberapa tahapan yaitu :

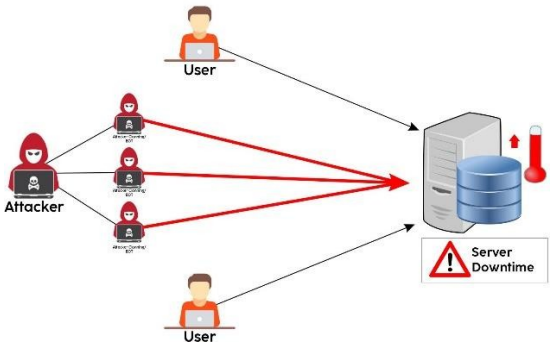
1. Tahap Analisis dan pengumpulan data
Tahap ini melibatkan pengumpulan dan analisis literature yang relevan mengenai teori otomata dan studi kasus serangan DDOS serta mengidentifikasi celah penelitian yang bisa diekporasi lebih lanjut.
2. Tahap Identifikasi Pola DDos
Pada tahap ini melakukan analisis data untuk mengidentifikasi karakteristik umum dari serangan Ddos seperti, volume lalu lintas yang tidak normal, distribusi sumber IP, dan pola waktu serangan. Langkah ini penting untuk menentukan parameter yang akan digunakan dalam model otomata.
3. Tahap Design
Pada tahap ini, merancang model automata yang dapat mendeteksi pola-pola serangan Ddos yang telah diidentifikasi, ini melibatkan pembuatan diagram status transisi automata yang mempresentasikan respon terhadap input data jaringan.
4. Tahap Implementasi
Pada tahap ini, mengembangkan alat pendeteksi Ddos berbasis model automata yang telah dirancang, proses ini mencangkup penulisan kode, pengujian unit, dan integrasi sistem menggunakan Bahasa pemograman yang sesuai.
5. Pengujian dan Evaluasi

Pada tahap menguji alat pendeteksi pada dataset serangan DdoS untukmengevaluasi akurasi dan performnya. Evaluasi mencangkup pengukuran Tingkat deteksi (*true positives*), kesalahan deteksi (*false positives* dan *false negatives*), serta efisiensi pemrosesan.

III. HASIL DAN PEMBAHASAN

3.1. Tahap Analisis dan pengumpulan data.
Tahap Pertama dalam penelitian ini adalah studi literatur, pada tahap ini kami melakukan kajian literatur yang mendalam mengenai serangan DdOS, khususnya pada penerapan teori otomata pada sebuah kemanan system untuk mengatasi serangan Ddos. Ini termasuk penelitian sebelumnya, buku, jurnal, dan sumber online yang relevan[7].

3.2. Tahap Identifikasi Pola Ddos
Tahapan ini mengidentifikasi karakteristik umum dari serangan Ddos terlebih dahulu. Serangan Ddos (Distributed Denial Of Service) bertujuan untuk melumpuhkan server atau jaringan dengan cara membanjiri lalu lintas internet[8]. Workflow Serangan ddos dapat dilihat pada gambar 1 sebagai berikut :



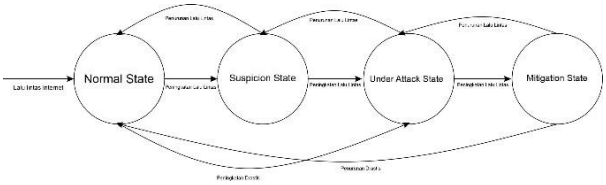
Gambar 1. Workflow Serangan Ddos

Keterangan gambar 1 :

1. Penyerang membanjiri lalu lintas jaringan dengan mengirim banyak data sehingga membuat lalu lintas jaringan terhambat dan User tidak dapat masuk ke dalam system jaringan,
2. Membanjiri jaringan dengan mengirim banyak request yang disediakan oleh *host* sehingga *request* dari user tidak dapat dilayani oleh layanan tersebut.
3. Dengan banyaknya reques dari user maka membuat kinerja server menurun.

3.3.Tahap Design

3.3.1. Pemodelan otomata
Pada tahap ini yaitu merancang model otomata dengan menggunakan FSA (*Finite State Automata*). *Finite State Automata* (FSA) merupakan mesin automata dari bahasa reguler. Suatu *Finite State Automata* memiliki state yang banyaknya berhingga, dan dapat berpindah- pindah dari suatu state ke state lain secara formal finite state automata dinyatakan oleh 5 tupel atau M (Q,∑,δ,S,F),Dimana :
Q = himpunan state / kedudukan
∑ = himpunan simbol input
δ = fungsi transisi
S = state awal / kedudukan awal (initial state)
F = himpunan state akhir[9].

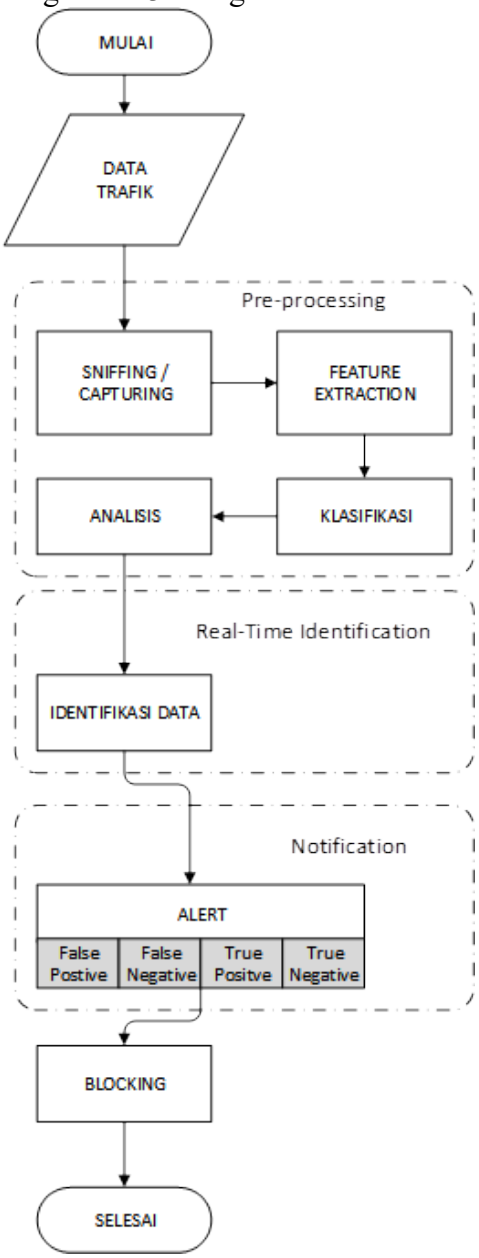


Gambar 2.Diagram FSA

Dimana {*normal, suspicion, under attack, mitigation*} adalah state, {*normal state*} merupakan state awal, {*mitigation state*} merupakan state akhir, dan {peningkatan, penurunan} = P adalah symbol input dengan read character.

3.3.2. Pemodelan Sistem Pendetekasi
Dalam pemodelan ini akan menggunakan *flowchart* sebagai Gambaran metode pendeteksi dan pencegahan terhadap serangan Ddos. *Flowchart* dapat dipahami sebagai langkah-langkah pemecahan masalah yang ditulis dalam simbol-simbol tertentu. Dan *flowchart* ini akan merepresentasikan alur dalam program

secara logika[10]. Flowchart metode pendeteksi dan pencegahan dapat dilihat pada gambar 3 sebagai berikut :



Gambar 3. Flowchat Pendeteksian dan Serangan DDos

3.4. Tahap Implementasi

Tahap ini mengimplementasikan alat deteksi Ddos sederhana menggunakan bahasa pemograman python, dengan tujuan agar lebih mudah untuk melakukan pengembangan selanjutnya [11] yang berbasis *Finite State Automata* (FSA) dan berikut adalah pseuducode :

```python
class DDoSDetector:
    def __init__(self):
        self.state = 'NORMAL'
        self.packet_count = 0
        self.suspicion_threshold = 50
        self.detection_threshold = 100
        self.mitigation_threshold = 150

    def process_packet(self, packet_size):
        if self.state == 'NORMAL':
            self.packet_count += 1
            if self.packet_count > self.suspicion_threshold:
                self.state = 'SUSPICION'
        elif self.state == 'SUSPICION':
            self.packet_count += 1
            if self.packet_count > self.detection_threshold:
                self.state = 'DETECTED'
        elif self.state == 'DETECTED':
            self.packet_count += 1
            if self.packet_count > self.mitigation_threshold:
                self.state = 'MITIGATION'
        elif self.state == 'MITIGATION':
            self.packet_count += 1

    def reset(self):
        self.state = 'NORMAL'
        self.packet_count = 0

    def is_suspicion(self):
        return self.state == 'SUSPICION'

    def is_ddos_detected(self):
        return self.state == 'DETECTED'

    def is_mitigation(self):
        return self.state == 'MITIGATION'

from scapy.all import sniff, IP


detector = DDoSDetector()

def packet_handler(packet):
    if packet.haslayer(IP):
        packet_size = len(packet)
        detector.process_packet(packet_size)
        if detector.is_suspicion():
            print("Suspicion of DDoS Attack!")
        if detector.is_ddos_detected():
            print("DDoS Attack Detected!")
        if detector.is_mitigation():
            print("DDoS Mitigation Started!")
            detector.reset()

sniff(prn=packet_handler, count=0)

```

Gambar 4. Pseuducode pendeteksi Ddos

Penjelasan *Pseuducode* :

Pada kode diatas mendefinisikan alat pendeteksi serangan Ddos menggunakan model *Finite State Automata* (FSA) dan menggunakan *library scapy* pada phyton untuk menangkap lalu lintas jaringan.dan penerapan Automata menggunakan model *Finite State Automata* (FSA) pada alat pendeteksi ini adalah pada bagian statenya yang berupa : *Normal state*, *Suspicion State*, *Under attack state/ detected state*, dan *mitigation state*.

1. *Normal State*

   Normal state terjadi jika *packet_count* tidak ada peningkatan secara signifikan atau pada kondisi stabil.

2. *Suspicion State*
   Dalam *suspicion state* terjadi apabila terjadi peningkatan pada *packet_count* yang melebihi *suspicion_threshold.*
3. *Under attack* / *Detected state*
   Under attack state terjadi apabila *packet_count* melebihi *setection threshold* bisa dikatakan serangan Ddos terdetekasi.
4. *Mitigation State*
   Mitigation state bisa dibilang penanganan jika serangan DDos terdeteksi.dan tindakan mitigasi bisa diinisiasi seperti : pembokliran IP, mengubah aturan *firewall*, dll)

IV. KESIMPULAN

Dari penelitian diatas dapat kami simpulkan bahwa penerapan teori otomata dalam pengujian keamanan jaringan terhadap serangan Ddos memberikan kerangka kerja yang efektif untuk menganalisis dan memitigasi ancaman terhadap server.Dengan menggunakan automata, kita dapat mengembangkan sistem deteksi yang lebih efisien dan respon yang lebih cepat, walaupun pada penelitian ini masih berada pada tahap perancangan dan mengimplementasi secara virtual ke dalam bahasa pemograman python tetapi hasil penelitian ini menunjukkan bahwa teori automata menggunakan *Finite State Automata* (FSA) sangat berguna sekali dalam peningkatan strategi dan pengujiankeamanan jaringan secara keseluruhan.

V. REFERENSI

[1] B. Triandi, “Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0,” 2019. [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom|Page477

[2] O. Rivaldi and N. L. Marpaung, “Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata,” vol. 8, no. 1, p. 2023.

[3] F. Nisa and S. Ramadona, “Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN,” vol. 5, no. 3, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[4] F. Titiani, S. Anggraeni Putri, W. Gata, and S. Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, “Penerapan Konsep Finite State Automata Pada Aplikasi Simulasi Vending Machine Jamu Tradisional,” *JURNAL INFORMATIKA*, vol. 7, no. 2, pp. 141–147, 2020, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji

[5] T. Akhir *et al.*, “Bentuk Serangan DoS (Denial of Service) dan DDoS (Distributed Deial of Service) pada Jaringan NDN (Named Data Network),” 2016.

[6] F. Antony and R. Gustriansyah, “Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata,” *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.

[7] Z. I. Sumayyah, S. Dimas, S. Permana, M. Tsabit, and A. Setiawan, “Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux,” *Journal of Internet and Software Engineering*, vol. 1, no. 2, pp. 1–14, 2024, doi: 10.47134/pjise.v1i2.2694.

[8] L. Ikhwanul Uzlah and R. Adi Saputra, “DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST,” 2024. [Online]. Available: https://bit.ly/CyberSecurityAttacks.

[9] A. S. Maulana, H. N. Azizah, and K. C. Kirana, “Ahmad Saufi Maulana: Implementasi Finite State Automata (FSA) Dengan Simulasi … IMPLEMENTASI FINITE STATE AUTOMATA (FSA) DENGAN SIMULASI VENDING MACHINE PADA APLIKASI ANDROID.” [Online]. Available: http://journal.uny.ac.id/index.php/jee/

[10] Khesya Nurhaliza, “MENGENAL FLOWCHART DAN PSEUDOCODE DALAM ALGORITMA DAN PEMROGRAMAN,” 2023.

[11] M. Misbahul Azis and Y. Azhar, “Analisa Sistem Identifikasi DDoS Menggunakan KNN Pada Jaringan Software Defined Network(SDN),” *REPOSITOR*, vol. 2, no. 7, pp. 915–922, 2020.