p-ISSN: 2301-6949
e-ISSN : 2715-5064

PENERAPAN METODE NIJ UNTUK ANALISIS SERANGAN DOS PADA PERANGKAT IOT

Singgih Mitro S[1*)], Dadan Sukma[2]
[1]Program Studi Informatika, Universitas Insan Cita Indonesia, Jakarta
[2]Jurusan Studi Informatika, Universitas Insan Cita Indonesia, Jakarta
[1]Jln. H,R Rasuna Said, Kota Jakarta Selatan, 12940, Indonesia
[2,3]Jln.H.R Rasuna Said, Kota Jakarta Selatan, 12940, Indonesia
email: singgihmitro @uici.ac.id, [2]dadansukma@uici.ac.id

Abstract **−− One of the problems of IoT is because many devices are connected to IoT in the industrial era 4.0, which ultimately distracts hackers from solving security mechanisms. One of the security factors of concern in this IoT device is a Denial of Service (DoS) attack on the Internet of Things (IoT) device network which results in a system being flooded with data continuously in a short time resulting in very dense network traffic. resulting in IoT device down. This study aims to apply the National Institute of Justice (NIJ) method in analyzing Denial of Service (DOS) attacks on Internet of Things (IoT) devices. The NIJ method includes stages such as preparation, incident handling, collection identification, collection, examination, analysis, reporting. The results of the study show that the NIJ method can be used to analyze DoS attacks on IoT devices and assist in taking action to prevent further attacks.**

Kata Kunci**Denial of Services (DoS), National Institute of Justice (NIJ), IoT.**

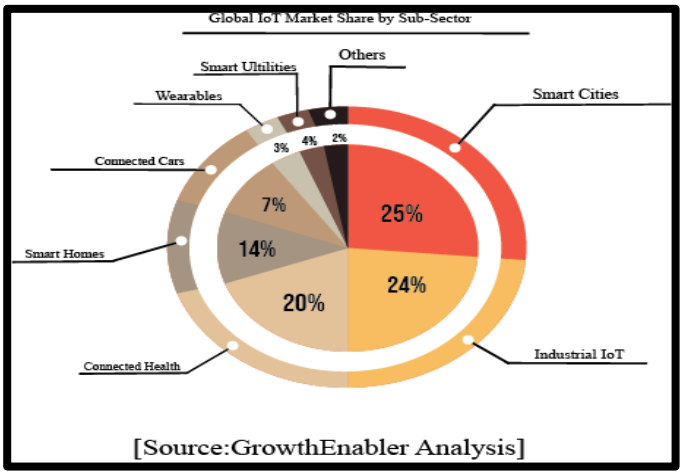
Abstrak **− Salah satu permasalahan IoT adalah karena banyaknya perangkat yang terhubung ke IoT di Era industri 4.0, pada akhirnya mengalihkan perhatian peretas dalam memecahkan mekanisme keamanan. Salah satu faktor keamanan yang menjadi perhatian dalam perangkat IoT ini adalah serangan *Denial of Service* (DoS) terhadap jaringan perangkat *Internet of Things* (IoT) yang mengakibatkan suatu sistem akan terbanjiri data secara terus menerus dalam waktu singkat yang mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga mengakibatkan perangkat IoT *down*. Penelitian ini bertujuan untuk menerapkan metode National Institute of Justice (NIJ) dalam menganalisis serangan Denial of Service (DOS) pada perangkat Internet of Things (IoT). Metode NIJ meliputi tahap-tahap seperti persiapan, penanganan insiden, pengumpulan identification, collection, examination, analisys, reporting. Hasil penelitian menunjukkan bahwa metode NIJ dapat digunakan untuk menganalisis serangan DoS pada perangkat IoT dan membantu dalam mengambil tindakan untuk mencegah serangan selanjutnya.**

Kata Kunci **– Denial of Services (DoS), National Institute of Justice (NIJ), IoT.**

I.PENDAHULUAN

Internet of Things merupakan istilah di masa depan dimana semua perangkat elektronik tersambung ke internet sehingga tercipta sebuah sistem yang memiliki kecerdasan sendiri yang sangat berguna dalam perkembangan teknologi.

Menurut laporan analisis GrowthEnabler tahun 2017, karena banyak perangkat yang terhubung ke IoT, pada akhirnya mengalihkan perhatian peretas dalam memecahkan mekanisme keamanan. Salah satu faktor keamanan yang menjadi perhatian dalam perangkat IoT ini adalah salah satu serangan bernama flooding.



Gambar 1 Perangkat IoT yang Terhubung Tahun 2016 – 2020

Belum lama ini terjadi bentuk serangan siber yang membuat suatu system tidak dapat diakses dengan membanjiri trafik jaringan dengan peningkatan jumlah perangkat IoT yang baru-baru ini, potensi kekuatan serangan DoS dengan menggunakan perangkat IoT berkembang pesat [1] DDoS mengganggu layanan dengan membuat kemacetan jaringan dan melumpuhkan fungsi normal dari komponen jaringan, yang bahkan lebih mengganggu IoT[2].

Untuk melakukan analisis serangan pada IOT, yaitu memanfaatkan aplikasi Wireshark yang memiliki fungsi menangkap paket data atau informasi dalam format Protocol yang berjalan dalam jaringan, sehingga data atau informasi tersebut langsung dapat dianalisis untuk memahami seberapa rawan suatu sistem untuk pelanggaran keamanan.

Dalam penelitian ini untuk proses analisis deteksi jenis serangan DoS pada pada perangkat Internet of Things (IoT) sehingga dilakukan akuisisi data pada IoT untuk menentukan karakteristik bukti digital melalui metode NIJ.

II.PENELITIAN YANG TERKAIT

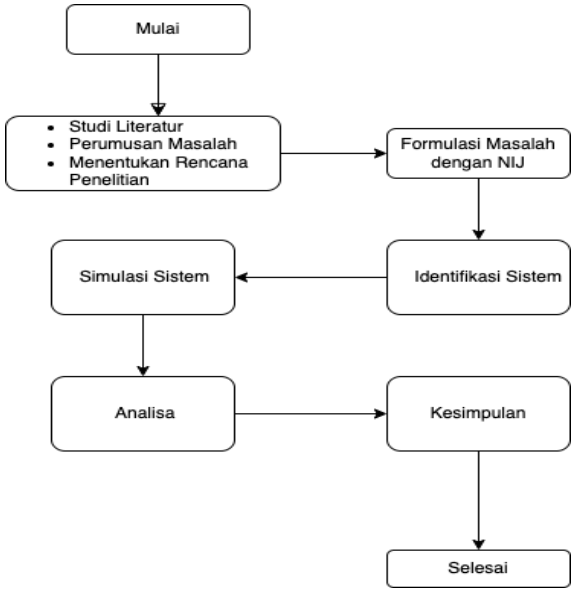
Beberapa penelitian dahulu berkaitan dengan Netwok forensic yang dilakukan oleh A. R. Caesarano and I. Riadi dengan judul " Network Forensics for Detecting SQL Injection Attacks using NIST Method yang bertujuan untuk mendeteksi serangan SQL Injection dan notifikasi serangan real time menggunakan email dengan pengembangan system web server menggunakan Snort untuk system deteksi dan menggunakan NIST untuk mendapatkan bukti digital. [3]

Penelitian lainya dilakukan oleh M. Alim, I. Riadi, and Y. Prayudi dengan judul *Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard* bertujuan untuk explorasi terhadap bukti digital yang bisa didapatkan dari Sistem Operasi Router untuk memperoleh informasi yang digunakan dalam penyelidikan forensic. [4]

Berdasarkan referensi diatas, penelitian ini akan difokuskan pada penerapan metode NIJ untuk analisis searangan DoS pada perangkat IoT yang bertujuan untuk menemukan barang bukti digital.

III. METODE PENELITIAN

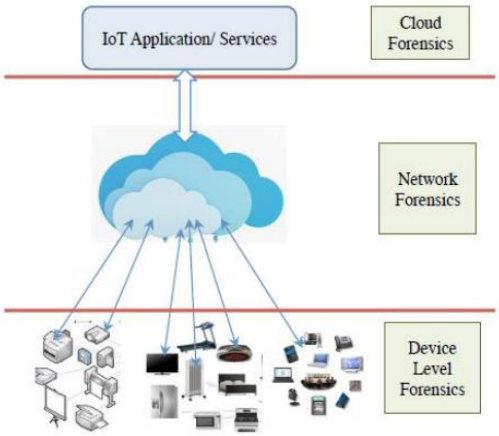
Pada penelitian ini menggunakan *flowchart* metodologi penelitian yang dapat dilihat pada Gambar 1.



Gambar 2 *Flowchart* Metodologi Penelitian

1. Forensik IoT

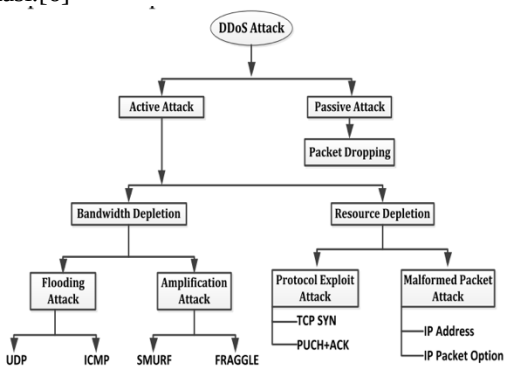
Forensik IoT adalah bagian dari digital forensik di mana semua fase untuk menemukan fakta yang terkait tentang kejahatan siber yang terjadi di lingkungan IoT. [5]



Gambar 3 Forensik IoT

2. DoS and DDoS Attack

Serangan DoS dapat dilakukan dengan menyalahgunakan perangkat, memanipulasi perangkat lunak dan aplikasi.[6]



Gambar 4 DoS Attack

3. National Institute Of Justice

Tahapan dari metode *National Institute of Justice* (NIJ) secara lengkap dipaparkan sebagai berikut: [7]

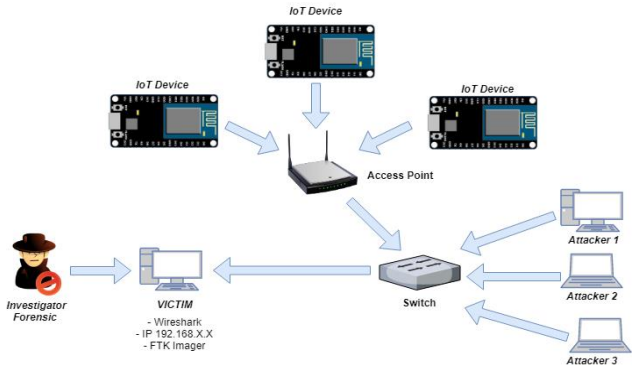
Gambar 5 *National Institute of Justice* (NIJ)

1. Tahap Identification, dentifikasi barang bukti digital yang dapat dipakai untuk mengungkap suatu kasus. Di dalamnya terdapat proses seperti pelabelan dan pencatatan barang bukti.
2. Collection, mengumpulkan barang bukti untuk mendukung penyelidikan mengungkap suatu kasus.
3. Examination, memeriksa data yang telah didapat secara forensik baik secara manual atau otomatis.
4. Analysis, bukti yang telah didapat dianalisis untuk mencari bukti tertentu yang berkaitan dengan kasus.
5. Reporting, dilakukan pelaporan dari hasil analisis temuan-temuan terkait dengan kasus dan sehingga diberikan kesimpulan dari analisis yang dilakukan.

IV. HASIL DAN PEMBAHASAN

1. Simulasi Serangan Dos Pada IoT

Berikut Rancangan simulasi serangan DoS pada IoT menggunakan LOIC, dan analisis serangan pada IoT menggunakan aplikasi Wireshark.



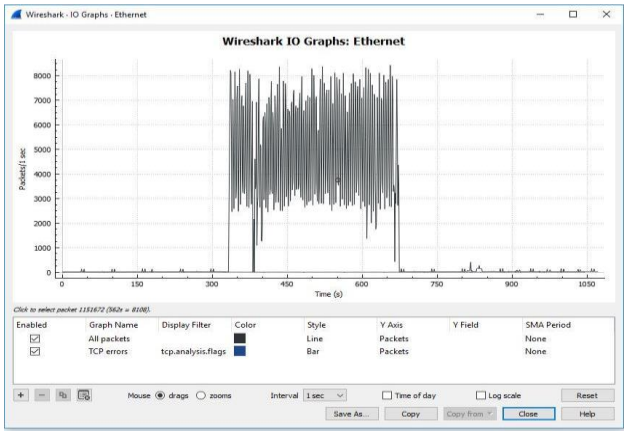
Gambar 6 Desain Analisis Serangan DoS pada IoT

2. Pengujian Menggunakan Aplikasi

Untuk pengujian serangan DoS pada IoT menggunakan aplikasi LOIC (*Low Orbit Ion Canon*) untuk mengetahui apakah serangan DoS berhasil menembus jaringan IoT.

Gambar 7 Aplikasi LOIC untuk Serangan DoS

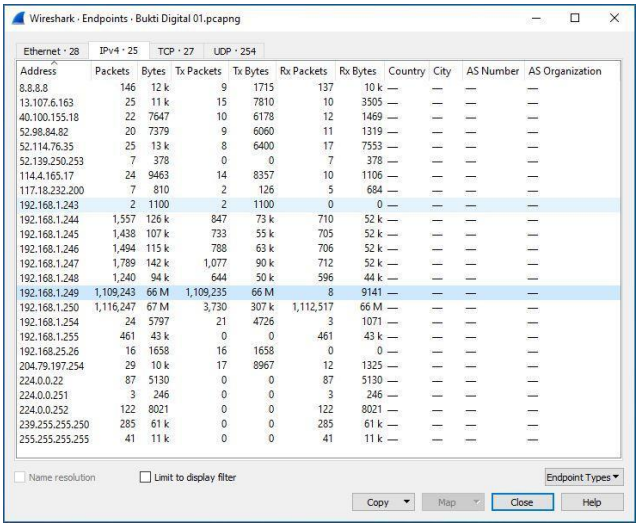
Setelah pengujian menggunakan aplikasi LOIC Berikut ini terlihat *traffic* yang *abnormal* yang telah terdeksi oleh *wireshark* kemudian penyidik mencari tau *attacker* yang mengirimkan *flooding* ke perangkat IoT.



Gambar 8 Serangan DoS pada IoT

Berdasarkan tampilan Gambar di atas, dapat dijelaskan bahwa aplikasi LOIC berhasil dijalankan dan siap melancarkan serangan ke jaringan IoT. Kemudian pada statistik *endpoint* terdapat jumlah serangan *flooding* bentuk TCP sejumlah 27 serangan dan UDP sebanyak 254 serangan. Tampilan hasil serangan pada Gambar berikut:

Gambar 9 Serangan DoS pada IoT



HASIL PENGUJIAN SERANGAN DOS PADA IOT

Tabel 1 Hasil Analisis Serangan DOS di IoT

No	Jenis Informasi Analisis	Keterangan
1	Serangan DoS pada IoT menggunakan aplikasi LOIC	Berhasil melakukan serangan secara bertubi-tubi pada perangkat IoT
2	Aplikasi *Wireshark* berhasil menangkap aktivitas lalu-lintas yang mencurigakan melalui *protocol* UDP	Diperoleh informasi bahwa adanya penyerang dengan serangan *flooding*.
3	Port serangan berhasil ditembus	Protocol UDP
4	Port Protocol Penyerang	59925

V. KESIMPULAN DAN SARAN

Setelah melakukan simulasi serangan DoS pada IoT, maka dapat ditarik beberapa temuan penelitian sebagai kesimpulan. Berikut kesimpulan penelitian ini:

1. Untuk pengujian serangan DoS pada perangkat IoT dilakukan ketika sistem jaringan sedang berjalan (hidup). Untuk mendeteksi serangan dan menganalisa serangan menggunakan Wireshark. Untuk akuisisi data menggunakan metode NIJ.
2. Saran yang dapat dilakukan untuk keperluan selanjutnya

adalah melakukan pengembangan terhadap tahapan–tahapan dalam menggunakan metode NIJ untuk kasus Internet Of Things (IoT) sehingga tahapan tersebut dapat digunakan pada seluruh barang bukti yang ditemukan di TKP.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis kepada Universitas Insan Cita Indonesia yang membantu ataupun memberikan dukungan terkait dengan penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] K. Hengst, "DDoS through the Internet of Things," *25th twente student conference on IT*, 2016.
[2] C. Zhang and R. Green, "Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network," *Proceedings of the 18th Symposium on Communications & Networking*, no. May, pp. 8–15, 2015.
[3] A. R. Caesarano and I. Riadi, "Network Forensics for Detecting SQL Injection Attacks using NIST Method," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 436–443, 2018.
[4] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int J Comput Appl*, vol. 180, no. 35, pp. 23–30, 2018, doi: 10.5120/ijca2018916879.
[5] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, pp. 279–284, 2015, doi: 10.1109/SCC.2015.46.
[6] B. Paharia, "DDoS Detection and Mitigation in cloud via FogFiter : a defence mechanism," *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, 2018.
[7] I. Riadi, R. Umar, and I. M. Nasrulloh, "ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.