BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Menurut artikel *Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends* pada tahun 2021, IoT analytics memperkirakan jumlah global perangkat IoT yang terhubung akan bertambah sebesar 9% untuk mencapai 12,3 miliar *endpoint* aktif. Pada tahun 2025, ada kemungkinan akan lebih dari 27 miliar koneksi IoT (Aldahmani et al. 2023). Dari situs web postel.co.id kominfo SDPPI (Sumber Daya dan Perangkat Pos dan Informatika) Yogyakarta menyebutkan potensi Internet of Things (IoT) terhadap peningkatan produktivitas di Indonesia pada tahun 2022 diperkirakan akan mencapai Rp 444 triliun, dengan 400 juta sensor (perangkat) saling terhubung, dan akan terus meningkat hingga sekitar Rp1.700 triliun pada tahun 2025 (Postel.co.id 2017). Artinya setiap tahun peningkatan perangkat IoT dan aktivitas penggunaan IoT cukup tinggi peningkatanya. Lembaga Pricewaterhouse Coopers (PwC) melakukan survei *Internet of Things* (IoT) terbanyak yang terpasang di rumah diantaranya lampu 65%, CCTV 58%, pengaman pintu 56%, pintu garasi 29%, perangkat dapur 20%, dan mobil 10% (Hariyadi, Setiawan, and Setiyadi 2021). Dari banyaknya objek perangkat IoT ternyata lampu cerdas menjadi alat yang banyak terpasang di rumah, dan faktanya rata- rata perangkat lampu cerdas sudah dilengkapi dengan teknologi nirkabel. Salah satunya sistem pengendali lampu rumah yang menggunakan aplikasi sebagai *remote control* (Ghaniy and Leksono 2023). *Remote contol* menjadi alat yang efisien dan memberikan kenyamanan bagi pengguna (Sitorus and Harahap 2023). Namun, justru potensi celah keamanan lebih mengancam, dan berbagai motif penyerang rumah cerdas lebih mudah. Maka diperlukan solusi untuk mendeteksi serangan pada ekosistem rumah cerdas (Hariyadi, Setiawan, and Setiyadi 2021). Ancaman keamanan ekosistem rumah dilakukan dengan melakukan pemasangan alat yang digunakan untuk mengintai pengguna rumah dan melakukan pengambilan data pribadi. Teknoligi IoT menjadi

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

salah satu senjata kejahatan yang banyak digunakan. Seperti yang terjadi pada sebuah kasus kejahatan IoT dengan menggunakan pengisi daya USB sebagai metode untuk mencuri data atau memasang malware. Kejahatan tersebut disebut *Juice jacking*. *Juice jacking* muncul sebagai risiko potensial menginfeksi pengguna dan berpotensi mencuri kata sandi mereka serta menyusup ke rekening bank (Statista 2020). Sehingga ancaman tersebut menjadi sebuah kemungkinan akan terjadi pada ekosisitem IoT sistem lampu cerdas.

Fenomena tersebut membentuk sebuah kesimpulan bahwa lampu merupakan objek sistem cerdas yang banyak terpasang pada rumah cerdas sehingga menjadi pemasok utama meningkatnya produktivitas IoT dan ancaman yang mengancam pada aktivitas IoT juga perlu diwaspadai. Dilihat dari hasil penelitian yang dilakukan oleh perusahaan Signify N.V bahwa jaringan nirkabel rentan diserang oleh *threat actor,* dan lampu cerdas termasuk dalam jaringan yang bersifat nirkabel sehingga menjadi bukti dan fakta menarik untuk pengujian penyerangan yang ada pada lampu cerdas tersebut. Pada sebuah jurnal ilmiah menyebutkan bahwa dari sekian banyak penyerangan yang terjadi, *malicious traffic* menjadi salah satu paling serius dalam dunia keamanan, dikarenakan *malicious traffic* dapat mentransfer berbagai macam kegiatan ilegal seperti penyebaran serangan *malware, Denial of Service* (DoS), dan *phising* (Hudzaifah, Sularsa, and Suchendra 2018). Malicious berpotensi terpasang pada sistem lampu cerdas. Sehingga beberapa sistem keamanan siber dikerahkan untuk melakukan pendeteksian untuk melindungi data *Smart Internet of Things* (SioT), komputer, dan aplikasi dari serangan dan akses tidak sah di lingkungan jaringan IoT (Shafiq et al. 2020). Sehingga penyerangan *malicious traffic* menjadi hal menarik juga untuk diteliti dengan dikaitkan pada rumah cerdas.

Dalam sebuah penelitian, terdapat bermacam cara dalam menangani masalah *malicious traffic* menggunakan HoneyPy dan Maltrail sebagai metode pembuktian. CentOs sebagai server tambahan dan Linux Mint sebagai server utama. Serangan yang dilakukan peneliti dalam penelitian tersebut menggunakan serangan DoS. Data yang dikumpulkan oleh Maltrail dianalisis menggunakan analisis deskriptif. Menurut hasil penelitian tersebut, HoneyPy dengan Maltrail

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

dapat menjadi tolak ukur peningkatan keamanan terhadap serangan sisi server. Penelitian lain melakukan rancangan model jaringan konvolusional HexCNN-1D yang menggabungkan mekanisme pemrosesan dan dinormalisasi. Dengan menambahkan modul mekanisme *Global Attention Block* (GAB) dan *Category Attention Block* (CAB), kemudian digunakan untuk mengklasifikasikan dan mengenali *malicious traffic* jaringan (Zhou et al. 2023). Akan tetapi tahap ini tidak cocok ketika diterapkan dalam pendeteksian *malicious traffic* pada lampu cerdas karena data yang digunakan tipe data teks dengan memfokuskan translasi pada bagian tertentu. Padalah pendeteksian *malicioust traffic* pada lampu cerdas hanya diperlukan alamat IP yang ada pada lampu untuk kemudian dilakukan pendeteksian lebih lanjut. Dari berbagai upaya penanganan *malicious traffic* diatas, peneliti bermaksud melakukan penelitian yang berbeda dari penelitian sebelumnya. Hal yang menjadi pembeda yaitu lampu cerdas sebagai objek penelitian yang akan dilakuakan analisi *malicious traffic* menggunakan aplikasi Maltrail. Masalah lain yang menjadi motivasi untuk mengangkat topik penelitian ini adalah pada sebuah penelitian yang menyebutkan bahwa *bloatware* merupakan *malware* yang sengaja ditanam pada *smartphone* untuk membuat sumber daya batrai, memori, ruang disk dan lainya menjadi terganggu dan mengakibatkan penyimpanan cepat penuh (Ozbay and Bicakci 2022) (Gaya et al. 2023). Sehingga penulis melakukan fokus mendeteksian yang dilakukan untuk mengetahui adanya *malware* yang sengaja ditanam pada lampu cerdas menggunakan metode *port mirroring* tersebut yang kemungkinan digunakan untuk melakukan penyerangan kepada pihak lain. Data dikumpulkan melalui *port mirroring*. *Port mirroring* diterapkan pada rangkaian topologi dan format data yang dikumpulkan adalah *packet capture*. Dataset jinak dan dataset berbahaya dikumpulkan secara terpisah. Kumpulan data jinak dikumpulkan segera setelah pemasangan jaringan karena merupakan dasar untuk mengidentifikasi jenis serangan lainnya. Informasi kontekstual paket mengenai protokol dan host ditangkap melalui aplikasi Maltrail .Topik ini belum pernah diteliti sebelumnya, sehingga akan menjadi bahan pengujian pertama dalam pendeteksian sisten IoT dan menjadi *insight* baru dan menambah daftar hitam

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

keamanan jaringan pada bidang IoT. Jika hasil dinyatakan tidak terdeteksi *malware* yang sengaja ditanam pada lampu cerdas, artinya lampu tersebut aman.

1.2 PERUMUSAN MASALAH

Penelitian ini terkait analisis *malicious traffic* pada IoT sistem lampu cerdas menggunakan aplikasi Maltrail. Peneliti menjelaskan proses implementasi Maltrail dalam menganalisis *malicious traffic* dengan menggunakan metode *port mirroring* untuk mengetahui adanya *malware* yang terindikasi tertanam secara langsung pada perangkat lampu cerdas yang terpasang pada *smart home*.

1.3 PERTANYAAN PENELITIAN

Berdasarkan perumusan masalah penelitian diatas, diuraikan menjadi beberapa pertanyaan penelitian, antara lain :

1. Bagaimana mengimplementasikan Maltrail dengan metode *port mirroring* dalam menganalisis *malicious traffic* pada lampu cerdas?
2. Bagaimana sistem dapat mengetahui adanya *malware* yang ditanamkan pada perangkat lampu cerdas?

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini yaitu untuk menambah daftar hitam deteksi *malicious traffic* pada lampu cerdas dan menambah *insight* baru pada pengguna agar lebih waspada terhadap serangan siber yang tidak hanya terjadi pada serangan dari luar tapi dapat diserang dari dalam yang sengaja ditanamkan.

1.5 MANFAAT HASIL PENELITIAN

Manfaat yang diperoleh dari penelitian adalah untuk menunjukan fakta baru terhadap pengguna IoT khususnya lampu cerdas. Mengingat lampu merupakan alat yang menjadi kebutuhan utama dalam sebuah rumah, dan dibandingkan alat IoT lainnya, lampu relatif murah dalam segi harga. Sehingga kemungkinan besar memiliki banyak pengguna. Oleh karena itu peneliti melakukan analisis adanya potensi *malicious traffic* jaringan yang keluar masuk pada lampu cerdas. Penelitian

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

ini diharapkan dapat memberikan wawasan dan kewaspadaan tentang ancaman *malicious traffic* yang ditimbulkan oleh perkembangan teknologi IoT atau mungkin saja dapat merugikan pihak lain akibat *malware* yang masuk atau sengaja ditanam dan adanya aktivitas kendali lampu cerdas yang mencurigakan sehingga dapat merugiakan pengguna.

PEPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA