BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah dan Kebutuhan

Internet of Things (IoT) merupakan konsep yang merujuk pada jaringan yang ada di perangkat fisik sehingga dapat terhubung dan berkomunikasi satu sama lain melalui internet. Perangkat IoT biasanya dilengkapi dengan sensor, perangkat lunak, dan teknologi lainnya sehingga mereka bisa mengumpulkan dan melakukan pertukaran data. IoT memungkinkan objek untuk diindra dan dikendalikan dari jarak jauh di seluruh infrastruktur jaringan yang ada, sehingga menciptakan peluang untuk integrasi yang lebih langsung dari dunia fisik ke dalam sistem berbasis komputer, dan menghasilkan efisiensi dan akurasi yang lebih baik. [1]

IoT telah menjadi bagian penting dari kehidupan modern, membantu berbagai sektor, mulai dari rumah tangga hingga industri, untuk meningkatkan efisiensi dan otomatisasi. [2] Namun, seiring dengan pesatnya adopsi perangkat IoT, risiko keamanan yang terkait dengan perangkat tersebut juga meningkat. Banyak perangkat IoT yang rentan terhadap serangan karena kelemahan dalam konfigurasi keamanan, seperti penggunaan kata sandi *default*, enkripsi yang lemah, dan kurangnya pembaruan perangkat lunak. Keamanan menjadi semakin penting karena serangan terhadap perangkat IoT dapat menyebabkan dampak yang luas, seperti pengambilalihan kendali perangkat, pencurian data, atau penggunaan perangkat untuk melakukan serangan *Denial of Service* (DoS). [3]

Perangkat IoT juga sering kali memiliki keterbatasan dalam hal daya komputasi dan baterai [4], yang menyulitkan implementasi solusi keamanan yang kompleks. Selain itu, rendahnya kesadaran pengguna akan pentingnya langkah-langkah keamanan turut memperburuk masalah ini. Oleh karena itu, perlu adanya alat *penetration Testing* yang khusus dirancang untuk perangkat IoT, yang mampu mengidentifikasi kerentanan dalam perangkat IoT dan menyimulasikan serangan untuk meningkatkan pemahaman pengguna terkait risiko keamanan. Salah satu teknologi yang mampu menyelesaikan masalah ini adalah Flipper Zero.

Flipper Zero merupakan sebuah alat yang berukuran kecil yang bertemakan lumba-lumba dan dapat berinteraksi dengan perangkat-perangkat digital lainnya. Flipper Zero pada dasarnya merupakan gabungan dari berbagai macam *hardware* sehingga alat ini dapat berkomunikasi melalui NFC, RFID, *Bluetooth*, dan *sub-GHz*. [5] Flipper Zero didesain agar mudah digunakan, dilengkapi dengan antarmuka yang mudah digunakan, tombol navigasi, layar kecil, dan maskot berupa lumba-lumba sehingga alat ini lebih interaktif dan menarik. Flipper Zero ini biasa

digunakan oleh praktisi keamanan untuk eksperimen sinyal sub-GHz, memindai *bluetooth* dan inframerah, dan juga mengsimulasi kartu akses seperti RFID dan NFC.

Hackbat merupakan alat *open-source* yang didesain untuk praktisi keamanan untuk bereksperimen dengan berbagai teknik *pen-testing*. Alat ini berbasis Raspberry Pi RP2040 dan memiliki NFC, WIFI, dan layar O*LED*. [17] [19] Sama seperti Flipper Zero, Hackbat dapat diprogram untuk menjalankan tugas praktisi keamanan untuk menguji keamanan sebuah alat dan jaringan.

1.2 Analisis Masalah

Masalah utama yang dihadapi dalam keamanan perangkat IoT adalah rentannya perangkat terhadap berbagai jenis serangan. Dari aspek teknis, kerentanan ini disebabkan oleh konfigurasi yang tidak aman, protokol komunikasi yang rentan, dan minimnya kemampuan perangkat dalam menangani enkripsi yang lebih kuat. Ditambah lagi, keterbatasan daya komputasi dan baterai mempersempit opsi untuk menerapkan solusi keamanan yang lebih banyak.

Penetration Testing adalah praktik pengujian untuk secara aktif menilai keamanan suatu sistem dengan merencanakan dan mengeksekusi semua kemungkinan serangan untuk menemukan dan mengeksploitasi kerentanan yang ada. [6] *Penetration Testing* penting dilakukan di perangkat IoT karena perangkat tersebut sering menangani data sensitif seperti informasi pribadi, data kesehatan, dan bahkan keuangan. Selain itu, *penetration Testing* juga dapat mencegah serangan terhadap IoT seperti *Man-in-the-middle* (MITM), DoS, dan serangan lainnya dengan cara mengidentifikasi celah keamanan yang dapat digunakan penyerang. [7] *Penetration Testing* juga dapat meningkatkan reputasi sehingga lebih banyak pengguna yang percaya untuk menggunakan suatu layanan.

Dari sisi pengguna, banyak yang masih kurang memahami risiko keamanan terkait penggunaan perangkat IoT. Hal ini menyebabkan pengguna sering kali mengabaikan langkah-langkah dasar seperti mengganti kata sandi *default* atau mengaktifkan enkripsi. Secara ekonomi, kerentanan pada perangkat IoT juga dapat menyebabkan kerugian finansial yang besar jika terjadi pencurian data atau serangan yang menargetkan infrastruktur. Oleh karena itu, alat yang dapat membantu pengguna memahami dan mengatasi kerentanan tersebut sebelum terjadi serangan nyata akan menjadi sesuatu yang berguna untuk lingkup ini.

1.2.1 Aspek Ekonomi

Kebocoran data pengguna dapat mengakibatkan beban finansial yang besar, meliputi biaya investigasi, pemulihan data, serta dampak buruk pada reputasi perusahaan. Sementara itu,

ketidakpatuhan terhadap regulasi keamanan data dapat memicu sanksi besar. Meskipun investasi awal dalam infrastruktur keamanan data mungkin tampak tinggi, langkah ini sebenarnya dapat menghemat biaya dalam jangka panjang dan membuka peluang untuk memperkuat kepercayaan pengguna, sekaligus memperluas pasar melalui reputasi perusahaan yang lebih baik [12].

Pemegang data dapat mengidentifikasi kelemahan sebelum terjadi serangan nyata dengan deteksi dini melalui perangkat *penetration-testing*. Perangkat ini membantu mengurangi biaya pemulihan setelah insiden yang umumnya mahal, seperti memperbaiki sistem, menangani pelanggaran data, dan membayar denda hukum atau kompensasi kepada pengguna yang dirugikan. Dengan ini, perusahaan dapat mengalokasikan anggaran untuk pencegahan daripada menyelesaikan masalah setelah insiden keamanan sistem terjadi dengan mengidentifikasi kerentanan lebih awal. Investasi pada perangkat *pen-testing* membantu mengoptimalkan pengeluaran operasional terkait keamanan, sehingga menjadi lebih efisien daripada harus menyiapkan dana besar untuk krisis keamanan yang tidak terduga.

1.2.2 Aspek Hukum

Kebocoran data yang terjadi pada suatu sistem, maka pengelola data tetap bertanggung jawab atas kerugian atas kebocoran data tersebut, terutama apabila terbukti bahwa suatu sistem tidak memiliki keamanan yang memadai. Apabila investigasi menemukan bahwa kebocoran data diakibatkan oleh kelalaian pengelola data dalam penerapan keamanan yang memadai, mereka dapat dikenakan sanksi. Sanksi ini bisa berupa denda, peringatan administratif, hingga tuntutan ganti rugi kepada pihak yang dirugikan.

Di Indonesia terdapat Pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur bahwa Pengendali Data Pribadi harus menyampaikan pemberitahuan tertulis kepada Subjek Data Pribadi dan lembaga dalam waktu paling lambat 3 x 24 jam apabila terjadi kegagalan perlindungan data pribadi. [15] Pengabaian aspek hukum ini dapat meningkatkan risiko reputasi dan biaya operasional bagi pengguna atau perusahaan yang gagal mengamankan data pengguna. Kemudian, ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) - UU No. 11 Tahun 2008 dan Perubahannya UU No. 19 Tahun 2016 yang mana pasal-pasal dalam UU ini mengatur tentang perlindungan data pribadi, kewajiban menjaga kerahasiaan, serta sanksi bagi pihak yang melakukan kejahatan siber, termasuk kebocoran data yang disebabkan oleh serangan siber. [16] Selain itu, di pasal 35 mengatakan bahwa pengendali data pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya. Lalu, pasal 36 menyatakan bahwa dalam melakukan

pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi. [15] Oleh karena itu, dibutuhkan perangkat untuk menguji keamanan sebuah sistem agar bisa mencari kelemahan suatu sistem dan menjaga agar data pengguna tetap aman.

1.2.3 Aspek Teknis

1.2.3.1 DoS

Denial of Service attack (DoS attack) adalah serangan siber dimana lalu lintas palsu terus dikirim ke *server* atau sistem sehingga sistem tersebut menjadi *down*. Tujuan dari serangan DoS adalah untuk membuat sebuah sistem tidak dapat diakses atau memberikan layanan. [5] Serangan DoS juga berdampak pada berbagai sektor seperti perbankan, *e-commerce*, media sosial, *cloud-services*, dan telekomunikasi, sehingga dapat memberikan kerugian finansial apabila tidak ada mitigasi yang baik. Apabila masalah DoS tidak segera diatasi, maka selain kerugian finansial akan terjadi kerusakan reputasi pada suatu sistem sehingga pengguna tidak mempercayai lagi suatu sistem dapat beroperasi dengan baik. Selain itu DoS juga bisa menyebabkan pengeluaran tambahan untuk meningkatkan kemampuan sumber daya yang mana hal itu memiliki biaya yang cukup tinggi. DoS juga bisa menjadi pengalih perhatian untuk serangan yang lebih besar sehingga hal tersebut bisa berdampak langsung terhadap suatu sistem atau layanan.

1.2.3.2 MITM

Man-in-the-middle (MITM) merupakan serangan dimana penyerang berada diantara dua pihak dan bisa mendengar, mengubah, bahkan membuat percakapan antara dua belah pihak. [8] Serangan ini berbahaya karena penyerang bisa mencuri data sensitif seperti informasi pribadi atau bahkan data industri. Selain itu data juga bisa dimanipulasi oleh penyerang yang mana hal itu akan merugikan pengguna yang terkena serangan MITM ini. Penyerang juga bisa mengambil alih suatu sistem apabila penyerang mendapatkan kredensial suatu sistem dan bisa melakukan kerusakan yang lebih besar terhadap suatu sistem. Selain itu, suatu penyedia layanan dapat mengalami kerugian karena telah melanggar privasi pengguna dan hal tersebut dapat diproses secara hukum sehingga penyedia layanan harus bertanggung jawab atas kerugian pengguna dari serangan MITM.

1.3 Analisis Solusi yang Ada

Setelah membandingkan solusi yang telah ada, kami menemukan beberapa poin penting yang dapat menjadi pertimbangan.

1. **Flipper Zero**

a. Keunggulan (*Strength*):
   i. Memiliki *User Interface* (UI) yang mudah digunakan dan menarik, dilengkapi dengan tombol navigasi dan layar kecil yang memungkinkan untuk akses cepat.
   ii. Mendukung banyak jenis komunikasi, termasuk NFC, RFID, *Bluetooth*, dan *sub-GHz*, sehingga mampu melakukan berbagai jenis uji keamanan.
   iii. Ukurannya kecil dan mudah dibawa, sehingga praktis digunakan di lapangan oleh pengguna.
   iv. Dapat digunakan untuk eksperimen sinyal sub-GHz, pemindaian *Bluetooth*, inframerah, serta mengsimulasikan kartu akses seperti RFID dan NFC.
   v. Memiliki daya tahan baterai yang cukup lama setelah melakukan pembaruan *firmware* sehingga perangkat dapat menyala hingga satu bulan.

b. Kekurangan (*Weakness*):
   i. Fitur keamanan canggih pada perangkat ini terbatas, khususnya untuk serangan yang membutuhkan kapasitas komputasi lebih besar atau analisis jaringan yang kompleks.
   ii. Harga perangkat Flipper Zero dapat menjadi faktor pembatas bagi pengguna pemula atau individu dengan anggaran terbatas.

c. Keterbatasan (*Limitation*):
   i. Flipper Zero lebih cocok untuk pengujian keamanan dasar dan mungkin kurang optimal untuk pengujian lanjutan atau penanganan data dalam skala besar.
   ii. Ketersediaan perangkat ini masih belum memadai di Indonesia

2. Hackbat

a. Keunggulan (*Strength*):
   i. Berbasis *open-source* dan menggunakan Raspberry Pi RP2040, sehingga memberikan fleksibilitas dalam hal pemrograman dan dapat dimodifikasi sesuai kebutuhan pengguna.
   ii. Dilengkapi dengan NFC, Wi-Fi, dan layar O*LED*, yang memperkaya kemampuan uji keamanan untuk mengakses jaringan atau perangkat yang terhubung ke internet.
   iii. Biaya lebih rendah dibandingkan Flipper Zero, yang membuatnya lebih terjangkau bagi praktisi pemula atau pengguna dengan anggaran terbatas.

b. Kekurangan (*Weakness*):
   i. Tidak memiliki antarmuka yang semudah Flipper Zero, sehingga membutuhkan pemahaman teknis lebih tinggi bagi pengguna pemula.
   ii. Karena berbasis *open-source*, stabilitas perangkat lunak bisa menjadi isu jika pengguna tidak melakukan pembaruan dan perawatan secara berkala.

c. Keterbatasan (*Limitation*):
   i. Karena berbasis pada Raspberry Pi, performa Hackbat mungkin terbatas pada tugas-tugas tertentu, terutama dalam pengetesan penetrasi yang membutuhkan daya komputasi tinggi.

Tabel 1.1 Estimasi harga pembuatan Hackbat

Perangkat	**Harga**
RP2040	Rp. 55.000
CC1101	Rp. 52.000
PN532	Rp. 50.000
128X64 O*LED* LCD *Display*	Rp. 40.000
ESP-12F *module*	Rp. 25.000
PCB	Rp. 291.795

Total	Rp. 513.795

Tabel 1.2 Perbandingan Spesifikasi

Fitur-fitur	**Flipper Zero**	**Hackbat**
Chipset	ARM Cortex-M4 dan ARM Cortex-M0+	*Dual core* ARM Cortex-M0+
Dapat dimodifikasi?	Ya	Ya
RFID	Ada	Tidak ada
WiFi	Tidak ada	Ada
NFC	Ada	Ada
Bluetooth Low Energy	Ada	Tidak ada
USB	Ada	Ada
Harga	Rp 7.224.999	Rp. 513.795

Berdasarkan *Tabel 1.2*, kami menemukan beberapa *pain point* dari kedua solusi tersebut. Kedua alat memiliki keterbatasan dalam hal daya komputasi, sehingga tidak cocok untuk menangani pengujian penetrasi yang kompleks dan hanya efektif untuk uji keamanan dasar. Dari segi aksesibilitas dan kemudahan penggunaan, Flipper Zero menawarkan antarmuka yang lebih ramah pengguna dan praktis, namun harganya relatif mahal. Sebaliknya, Hackbat lebih terjangkau secara finansial tetapi kurang intuitif bagi pengguna pemula, sehingga membutuhkan pemahaman teknis yang lebih tinggi untuk dapat digunakan secara efektif.

Gambar 1.1 Desain PCB Hackbat

Dengan pertumbuhan eksponensial penggunaan perangkat IoT, masalah keamanan menjadi sangat penting. Perangkat IoT sering kali rentan terhadap serangan akibat konfigurasi yang tidak aman dan kurangnya kesadaran pengguna, yang dapat mengakibatkan pencurian data dan kerusakan reputasi.

Kompleksitas masalah ini diperparah oleh keterbatasan teknis perangkat IoT yang umumnya memiliki daya komputasi dan baterai yang rendah, sehingga menyulitkan penerapan solusi keamanan yang efektif. Selain itu, tingginya risiko serangan seperti DoS dan MITM menunjukkan bahwa penting bagi pengguna untuk memahami risiko ini dan mengambil langkah mitigasi yang baik.

Setelah menganalisis solusi yang ada, seperti Flipper Zero dan Hackbat, mengungkapkan beberapa *pain point*. Keduanya memiliki batasan dalam hal kemampuan komputasi, serta tingkat kemudahan penggunaan yang berbeda. Meskipun Flipper Zero menawarkan antarmuka yang menarik, harganya bisa menjadi kendala bagi pengguna baru, sementara Hackbat yang lebih terjangkau memerlukan pemahaman teknis lebih tinggi.