Volume 6 Nomor 1 Januari 2021

INFORMASI INTERAKTIF

JURNAL INFORMATIKA DAN TEKNOLOGI INFORMASI

PROGRAM STUDI INFORMATIKA – FAKULTAS TEKNIK -UNIVERSITAS JANABADRA

INFORMASI INTERAKTIF	Vol. 6	No. 1	Hal. 1 - 55	Yogyakarta Januari 2021	ISSN 2527-5240

INFORMASI INTERAKTIF

ISSN 2527-5240

DEWAN EDITORIAL

Alamat Redaksi : Program Studi Informatika Fakultas Teknik
Universitas Janabadra
Jl. Tentara Rakyat Mataram No. 55-57
Yogyakarta 55231
Telp./Fax : (0274) 543676
E-mail: informasi.interaktif@janabadra.ac.id
Website : http://e-journal.janabadra.ac.id/

Frekuensi Terbit : 3 kali setahun

JURNAL INFORMASI INTERAKTIF merupakan media komunikasi hasil penelitian, studi kasus, dan ulasan ilmiah bagi ilmuwan dan praktisi dibidang Teknik Iinformatika. Diterbitkan oleh Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra di Yogyakarta, tiga kali setahun pada bulan Januari, Mei dan September.

INFORMASI INTERAKTIF ISSN 2527-5240

DAFTAR ISI

ISSN 2527-5240

PENGANTAR REDAKSI

Puji syukur kami panjatkan kehadirat Allah Tuhan Yang Maha Kuasa atas terbitnya JURNAL INFORMASI INTERAKTIF Volume 6, Nomor 1, Edisi Januari 2021. Pada edisi kali ini memuat 7 (tujuh) tulisan hasil penelitian dalam bidang informatika.

Harapan kami semoga naskah yang tersaji dalam JURNAL INFORMASI INTERAKTIF edisi Januari tahun 2021 dapat menambah pengetahuan dan wawasan di bidangnya masing-masing dan bagi penulis, jurnal ini diharapkan menjadi salah satu wadah untuk berbagi hasil-hasil penelitian yang telah dilakukan kepada seluruh akademisi maupun masyarakat pada umumnya.

Redaksi

IMPLEMENTASI MODEL *FORENSIC AWARE ECOSYTEM FOR IOT* (FAIOT) PADA PURWARUPA RUMAH PINTAR BERBASIS *INTERNET OF THINGS* (IOT)

Eri Haryanto [1], Agustin Setiyorini[2]

[1,2] Program Studi Informatika, Fakultas Teknik, Universitas Janabadra
Email : [1]eri@janabadra.ac.id, [2]agustin@janabadra.ac.id

ABSTRACT

The internet network that connects many computers in the world has now reached almost all regions in Indonesia. IoT is a technology concept consisting of objects that are connected to each other via an internet network that has a special address and can communicate with each other which gives birth to various types of smart systems such as smart homes, smart farms, smart cities, smart building, smart health, smart transport, and smart environments. other.

This study designs a smart home application model that is designed in such a way as to be equipped with the FAIoT model. This research has a specific objective, namely to apply the FAIoT model to a smart home application prototype, then run a case simulation on a smart home application and analyze the resulting digital artifacts as a consideration in proving a case. Based on the results of the analysis and observations of the forensic IoT devices in the form of two smart houses that were targeted by the attackers, it shows that system activity is stored properly on the FAIoT platform. The results of the analysis prove that the attack on IoT devices in the form of two smart houses can reveal the facts of the case based on findings that are used as digital evidence. In addition to the fact findings from the cases that occurred in this study, the Internet of Things (IoT) environment with the FAIoT Model has been successfully developed in this study, which can be used as research objects.

Keywords: *Smarthome, Internet of Things, IoT forensic, IoT Security*

1. PENDAHULUAN

Jaringan internet yang menghubungkan banyak komputer di dunia saat ini sudah menjangkau hampir seluruh wilayah di Indonesia. Saat ini jaringan internet tidak hanya menghubungkan komputer yang berupa personal komputer. Internet telah menjadi *backbone* transmisi data dari berbagai perangkat yang dikoneksikan ke jaringan internet. Salah satunya adalah perangkat *Internet of Things* (IoT).

IoT adalah konsep teknologi yang terdiri dari objek-objek yang saling terkoneksi melalui jaringan internet yang memiliki alamat khusus dan dapat saling berkomunikasi satu sama lain untuk memberikan suatu layanan tertentu [1]. Dengan munculnya teknologi IoT, menjadi cikal bakal berkembangnya berbagai teknologi dengan sistem cerdas seperti *smart home, smart building, smart transport, smart health, smart city,* dan lingkungan *smart* lainnya. Ide utama dari perangkat IoT adalah adanya perangkat canggih yang dapat berjalan otomatis yang memiliki koneksi aman dalam pertukaran data bersumber dari sensor-sensor yang terpasang pada perangkat IoT [2].

Seiring berjalannya waktu jumlah perangkat IoT yang terpasang dan terhubung ke dalam jaringan internet terus bertambah. IoT sebagai teknologi yang terbuka dan memiliki konektivitas dengan jaringan internet merupakan obyek yang tidak lepas dari ancaman serangan *cyber*. Pada kasus yang berkaitan dengan kejahatan *cyber* dibutuhkan peran investigator forensik untuk membantu mengungkap fakta kasus. Tugas investigator forensik akan sangat berat pada kasus yang melibatkan perangkat IoT. Hal tersebut dikarenakan belum adanya *tool* khusus dan prosedur yang sesuai untuk melakukan forensik digital perangkat IoT. Sehingga investigator forensik kesulitan dalam mendapatkan artefak digital karena terlalu banyak perangkat yang harus dianalisis forensik pada investigasi kasus yang menyangkut perangkat *internet of things*. Keberagaman jenis perangkat dan teknologi IoT akan memunculkan tantangan baru bagi investigator forensik [3].

Selain keberagaman jenis perangkat pada teknologi IoT, lingkungan kerja perangkat yang tidak jelas batas-batas sistemnya menjadi kendala dalam investigasi kasus yang melibatkan perangkat IoT. Menurut [4]

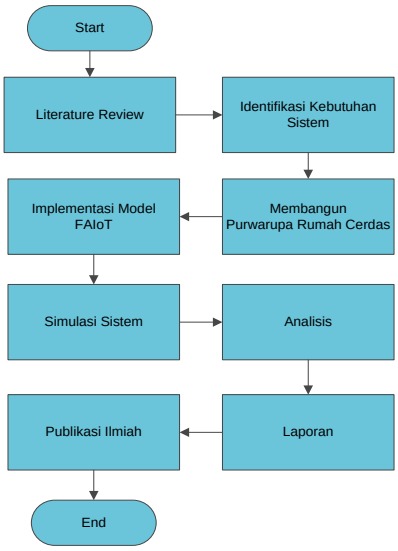
Perangkat IoT melibatkan tiga unsur forensik pada proses investigasinya, yaitu *cloud forensic, network forensik*, dan *device level forensic*. Saat ini alat forensik dan prosedur forensik yang ada belum dapat digunakan untuk menangani berbagai bentuk dari perangkat IoT. Model *Forensics-aware* IoT (FAIoT) diusulkan menjadi salah satu model yang dapat mendukung investigator forensik pada *environment* IoT.

Berdasarkan uraian di atas, pada penelitian ini dapat dirumuskan masalah yaitu bagaimana menerapkan Model FAIoT (*Forensic Aware for* IoT) pada purwarupa rumah cerdas yang berkonsep Internet of Things (IoT). Tujuan khusus dari penelitian ini yaitu membangun purwarupa rumah cerdas dan menerapkan Model FAIoT untuk memudahkan proses investigasi ketika terjadi tindakan kejahatan pada perangkat IoT.

Penelitian ini penting untuk dilakukan karena dengan penerapan model FAIoT pada purwarupa rumah cerdas dapat diketahui bukti digital dalam pengungkapan fakta kasus. Sehingga investigator forensik tidak perlu melakukan analisis forensik pada level device yang terpasang di berbagai tempat. Investigator forensik dapat lebih fokus pada analisis barang bukti digital.

2. METODE PENELITIAN

Pada gambar di bawah ini dapat dilihat tahapan penelitian yang akan dilakukan.



Gambar 1. Tahapan Penelitian

Literature review

Literatur review dilakukan untuk mendapatkan informasi terbaru terkait topik yang diteliti didapatkan dari referensi buku, artikel, dokumen, atau bahan tertulis lain yang berupa laporan hasil penelitian terdahulu yang telah dipublikasikan. Referensi tersebut didapatkan dari sumber bersifat *online* dan *offline*.

Identifikasi Kebutuhan Sistem

Merupakan tahap persiapan dalam implementasi pada *environment* perangkat *internet of things* yang akan digunakan sebagai objek penelitian. Terdiri dari dua tahapan identifikasi yaitu objek penelitian serta alat dan bahan.

Dalam penelitian ini dibutuhkan sebuah lingkup penelitian yang mendukung dilakukannya penelitian. Pada penelitian ini akan dibangun *prototype* perangkat *Internet of Things* berupa rumah cerdas.

Dalam membangun *environment* sebagai objek penelitian, dibutuhkan dukungan perangkat keras dan perangkat lunak. Kebutuhan perangkat keras antara lain sebagai berikut: Raspberry pi Board, Sensor Suhu DHT22, LED, Photo Resistor (Sensor Cahaya), Modul Sensor Hujan MD-0127 dan beberapa komponen lain untuk membangun purwarupa rumah cerdas.

Kebutuhan Kebutuhan perangkat lunak antara lain sebagai berikut: Sistem Operasi Centos untuk *web server platform* IoT dan Sistem Operasi Raspbian yang ditanamkan pada Raspberry pi 3 Model B+ *board*.

Membangun Purwarupa Rumah Cerdas

Pada tahap ini akan dibangun *environment* perangkat *internet of things* berupa *smart home* untuk simulasi sistem. Perangkat IoT *smart* home akan dipasang pada purwarupa miniatur rumah cerdas yang didesain untuk otomatisasi rumah tersebut. Perangkat IoT akan dibangun berbasis *single board computer* Raspberry Pi *Board*.

Implementasi Model FAIoT

Pada tahap ini model FAIoT akan diterapkan di dalam sistem rumah cerdas, berbagai set fungsi akan ditambahkan pada perangkat lunak rumah cerdas sehingga setiap *state* kondisi dari pembacaan sensor, *registry log*, serta *log* jaringan akan dapat dipantau dan disimpan ditempat khusus berupa repositori barang bukti. Dalam implementasi model FAIoT juga dilengkapi API agar investigator dapat mengakses barang bukti melalui API.

Simulasi Sistem

Merupakan tahap dilakukannya simulasi langsung pada sistem yang menjalankan perangkat IoT dengan memastikan *environment* berjalan sesuai dengan fungsinya.

Analisis

Pada tahap ini dilakukan investigasi dengan tujuan menemukan barang bukti ketika terjadi simulasi kasus. Dalam melakukan investigasi, menggunakan proses forensik digital dasar yang meliputi fase *collection*, *examination*, *analisa*, dan *reporting* yang berfokus pada repositori barang bukti.

Laporan

Merupakan tahapan pembuatan laporan dari hasil penelitian implementasi Model FAIoT serta laporan analisis terhadap simulasi sistem yang dilakukan.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Sistem

Analisis sistem bertujuan untuk mengidentifikasi permasalahan yang terdapat dalam aplikasi yang akan dibangun meliputi Identifikasi Kebutuhan Sistem.

Langkah awal untuk membangun environment internet of things (IoT) dilakukan identifikasi kebutuhan sistem yang terdiri atas kebutuhan perangkat keras dan kebutuhan perangkat lunak.

Pada penelitian ini dibangun *environment* IoT yang terdiri atas dua rumah cerdas yang diterapkan model FAIoT didalamnya. Kebutuhan perangkat keras dalam penelitian ini dapat dilihat pada tabel 1 di bawah ini.

Tabel 1. Kebutuhan Perangkat Keras

Perangkat	Komponen/Spesifikasi
Purwarupa rumah cerdas	• Raspberry Pi Board (2 unit) • Modul Sensor Suhu DHT22 (2 unit) • Modul Sensor Hujan (2 unit) • Lampu LED (8 unit) • Photo Resistor (LDR) (2 unit)
Server Hosting Platform *Internet of Things*	• Alamat domain (2 unit) • Media penyimpanan 1 GB

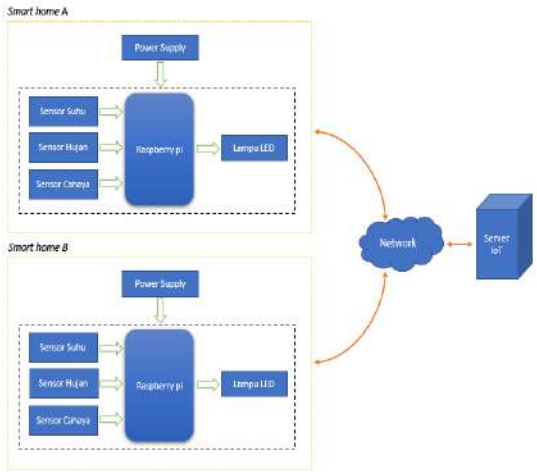
Dari hasil identifikasi kebutuhan perangkat keras dapat dilihat bahwa sistem rumah cerdas akan diotaki raspberry pi. Raspberry pi merupakan modul papan sirkuit tunggal yang dapat diinstall sistem operasi dan aplikasi yang banyak digunakan untuk membangun *embedded* system [5].

Selain kebutuhan perangkat keras dalam membangun environment IoT sebagai obyek penelitian juga dilakukan identifikasi kebutuhan perangkat lunak. Kebutuhan perangkat lunak dalam membangun environment IoT dapat dilihat pada Tabel 2.

Tabel 2. Kebutuhan Perangkat Lunak

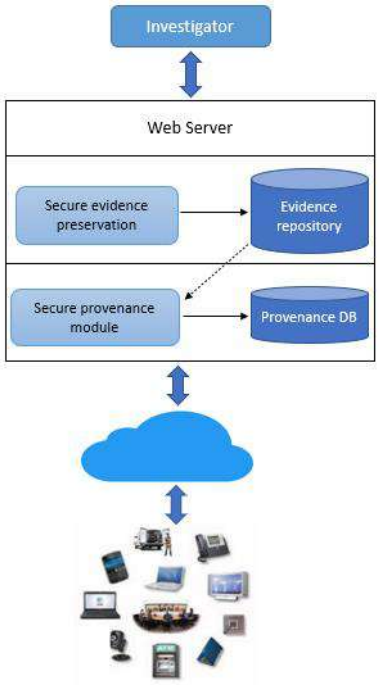
Perangkat	Kebutuhan
Perangkat lunak pada Server Hosting	• Raspberry Pi Board (2 unit) • Modul Sensor Suhu DHT22 (2 unit) • Modul Sensor Hujan (2 unit) • Lampu LED (8 unit) • Photo Resistor (LDR) (2 unit)
Perangkat lunak pada Raspberry pi Board	• Sistem Operasi Raspbian
Perangkat Lunak Editor	• Sublime Text 3 • Notepad++
Perangkat lunak pada komputer attacker	• Sistem Operasi Windows 10 • Browser

Pada Gambar 1 menunjukkan diagram blok sistem rumah cerdas yang dibangun pada penelitian ini.



Gambar 2. Diagram Blok Infrastruktur IoT Rumah Cerdas

Purwarupa rumah cerdas dirancang dengan menerapkan konsep *Forensic aware IoT* (FAIoT). Dengan FAIoT akan membantu investigator forensik dalam kegiatan pengambilan barang bukti ketika terjadi serangan terhadap perangkat atau infrastruktur IoT. Di bawah ini adalah model FAIoT yang diterapkan pada purwarupa.



Gambar 3. Model *Forensic aware for IoT* (FAIoT) [4]

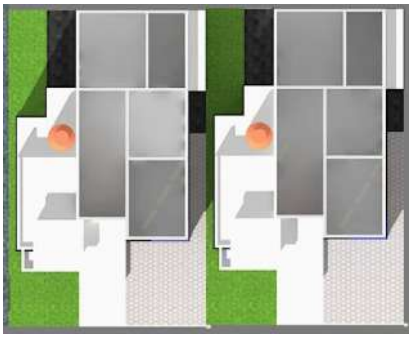
Pada model FAIoT seluruh aktifitas perangkat akan direkam atau disimpan dalam sebuah database khusus yang akan menyimpan seluruh aktifitas berupa data log. Data log bisa menjadi calon *evidence* (barang bukti) ketika terjadi tindak ilegal pada perangkat. Data log disimpan di sebuah database yang disebut *evidence repository*. Data log disimpan dengan enkripsi yang hanya dapat dibuka oleh agen legal yang memiliki kunci enkripsi tersebut. Untuk menjamin integritas data log pada *evidence repository* maka aktifitas akses ke database akan direkam pada sebuah sistem penyimpanan yang disebut *Provenance* DB.

Membangun Purwarupa

Pada penelitian ini purwarupa rumah cerdas yang menjadi obyek penelitian dirancang untuk memiliki fungsi seperti di bawah ini:Pemilik rumah dapat mematikan dan menyalakan lampu rumah dari jarak jauh.

a. Lampu rumah akan otomatis menyala ketika kondisi luar rumah sudah gelap karena mendung dan kondisi waktu sudah malam.
b. Pemilik rumah dapat memonitor suhu ruangan di dalam rumah setiap saat.
c. Pemilik rumah dapat memonitor kondisi di rumah apakah sedang terjadi hujan dari jarak jauh.
d. Pemilik rumah dapat menjalankan fungsi-fungsi di atas cukup melalui *smartphone*.

Berdasarkan data kebutuhan di atas selanjutnya peneliti membuat desain rumah cerdas dengan visualisasi tida dimensi. Desain rumah cerdas terdiri atas dua rumah dengan bentuk dan sistem yang sama. Dalam tahap simulasi kedua sistem rumah cerdas tersebut akan diretas dan untuk pengungkapan kasusnya peneliti akan melakukan pembangkitan barang bukti digital yang tersimpan pada database FAIoT.



Gambar 4. Desain *Layout* Puwarupa Rumah Cerdas Tampak Atas

Berdasarkan desain layout pada gambar di atas, peneliti membuat desain dalam bentuk tiga dimensi. Kedua rumah tersebut akan

dipasangkan perangkat IoT yang sudah lengkap dengan *platform* IoT dan *platform* FAIoT.

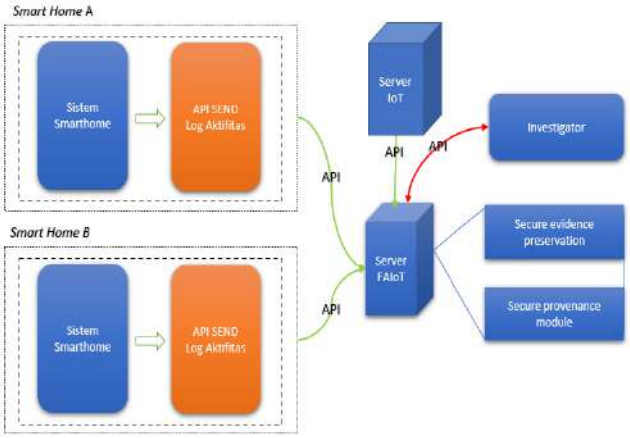
Gambar 5. Desain *Layout* Puwarupa Rumah Cerdas Tiga Dimensi

Implementasi FAIoT pada purwarupa rumah cerdas tidak pada sisi perangkat keras, namun pada sisi perangkat lunak. Agar perangkat keras yang telah dirancang dapat berfungsi sesuai dengan diharapkan maka harus ada perangkat lunak yang dimasukkan ke dalam sistem operasi raspberry pi dan server IoT. Pada penelitian ini peneliti membangun perangkat lunak tersebut dengan dilengkapi dengan implementasi model FAIoT.

Dengan model FAIoT, perangkat IoT perangkat lunak IoT akan mengirimkan data-data ke *platform* IoT dan juga akan mengirimkan data log aktifitas ke dalam *platform* FAIoT berbentuk aplikasi yang terinstall pada server. Log aktifitas hanya dapat dibuka oleh agen investigator forensik yang memiliki ijin (otoritas).

Data yang tersimpan di *platform* FAIoT akan disimpan dalam bentuk hash terenkripsi. Sehingga hanya dapat dibuka dengan kunci khusus yang telah disiapkan. Untuk menjaga integritas data log yang tersimpan di dalam database FAIoT, maka dalam *platform* model ini juga dilengkapi dengan aplikasi khusus yang selalu menyimpan log aktifitas akses terhadap data *evidence* di dalam *platform* FAIoT.

Dengan data log berlapis ini diharapkan integritas barang bukti bisa valid untuk pembuktian jika terjadi kasus.

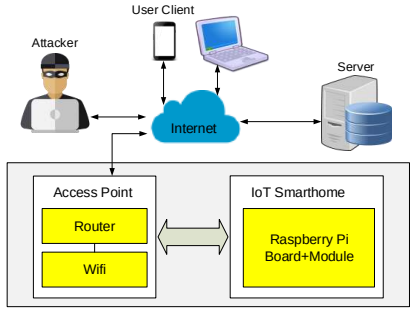


Gambar 5. Blok Diagram Implementasi FAIoT pada Perangkat Lunak Rumah Cerdas

3.2 Analisis Model Proses Forensik

Proses forensik digital untuk melakukan forensik pada sistem IoT yang dilengkapi model FAIoT ini menggunakan analisis model proses forensik antara lain: (1) *Collection*, (2) *Examination*, (3) *Analysis*, dan (4) *Reporting*. Dengan menggunakan analisis model forensik akan menjamin barang bukti digital yang ditemukan dapat digunakan untuk pembuktian kasus sampai di meja persidangan [5].

Analisis model proses forensik akan dilakukan untuk mengungkap fakta berdasarkan simulasi skenario kasus. Bagan simulasi kasus pada perangkat IoT rumah cerdas dapat dilihat pada gambar di bawah ini.

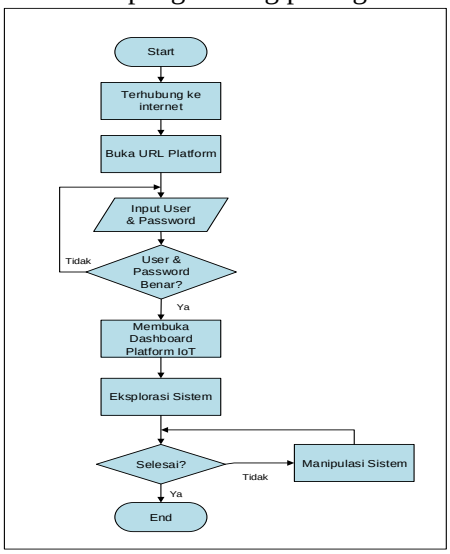


Gambar 6. Simulasi Kasus Pada Rumah Cerdas

Pada gambar di atas terlihat bahwa *attacker* masuk ke dalam sistem melalui jaringan internet dan menyasar ke dalam *environment* rumah cerdas berbasis IoT. Dalam hal ini *attacker* telah mendapatkan alamat URL portal *platform* IoT sebagai *controller* sistem rumah cerdas. Melalui celah *default account* pada portal, *attacker* telah berhasil masuk ke dalam *platform* IoT sehingga dapat melakukan

eksplorasi perangkat-perangkat IoT yang terdaftar di dalam platform tersebut.

Default *account* yang merupakan kombinasi dari user dan password seringkali menjadi celah keamanan yang sangat rentan dapat disusupi oleh *attacker*. Dalam membangun environment IoT tentunya sisi keamanan sangat penting untuk diperhatikan. Sehingga langkah-langkah untuk *hardening security* pada perangkat IoT menjadi prioritas dari vendor-vendor pengembang perangkat IoT.



Gambar 7. Alur Skenario Penyerangan pada Rumah Cerdas

Gambar 3 menunjukkan alur skenario kasus yang terjadi. Penyerang mengawali aksinya dengan terhubung ke jaringan internet, dilanjutkan membuka alamat URL *platform* IoT (rumah cerdas) berada. Setelah terbuka form login *platform* IoT, penyerang melakukan percobaan login dengan menggunakan kombinasi akun (*username* dan *password*) *default* yang umum digunakan oleh banyak pengembang sistem.

Pada penelitian ini secara default *platform* IoT menggunakan akun standar untuk mengakses portal tersebut yaitu:

Tabel 3. Akun default *platform* IoT

Field	Value
Username	administrator
Password	administrator

Detail tahapan skenario penyusupan oleh *attacker* (penyerang) dijelaskan di bawah ini:

1. Penyerang menghidupkan komputernya untuk terhubung ke jaringan internet global.
2. Penyerang telah mengetahui alamat URL platform IoT hasil dari pencarian menggunakan mesin pencari.
3. Alamat URL platform IoT diakses untuk mengetahui apakah alamat tersebut masih aktif.
4. Sistem akan menampilkan login form sebagai pintu masuk ke dalam *platform* IoT.
5. Penyerang mencoba-coba kombinasi username dan password default yang secara umum digunakan oleh pengembang sistem.
6. Dengan kombinasi username dan password yang sesuai selanjutnya penyerang dapat masuk ke dalam platform IoT.
7. Akan ditampilkan dashboard utama dari sistem, yang menampilkan perangkat IoT (rumah cerdas) yang terdaftar dan terhubung dengan platform.
8. Penyerang melakukan eksplorasi ke dalam sistem untuk melakukan tindakan ilegal dengan memanipulasi konfigurasi pada perangkat rumah cerdas.

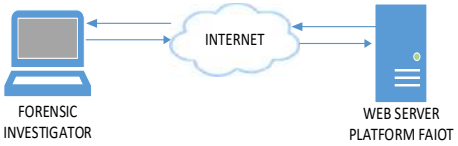
Dengan dilakukan analisis forensik diharapkan dapat ditemukan bukti digital beserta karakteristik dari adanya penyerangan dan penyusupan ke dalam sistem rumah cerdas berbasis *Internet of Things* yang menjadi obyek penelitian pada penelitian ini.

Tabel 8. Peralatan Yang Diperlukan Untuk Proses Investigasi Perangkat IoT berbasis FAIoT

Peralatan	Kegunaan
Perangkat Komputer	Digunakan untuk proses akuisisi, pemeriksaanm analisis dan reporting hasi forensik perangkat IoT
FAIoT Hunt	Merupakan aplikasi yang digunakan untuk melakukan proses analisis terhadap perangkat IoT.

1. Tahap Pengumpulan (Collection)

Tahap ini merupakan tahap awal dalam proses forensik yang bertujuan mengumpulkan barang bukti digital yang berhubungan dengan kasus yang terjadi.



Gambar 8. Proses Akuisisi Barang Bukti Digital dengan FAIoT (*Live System*)

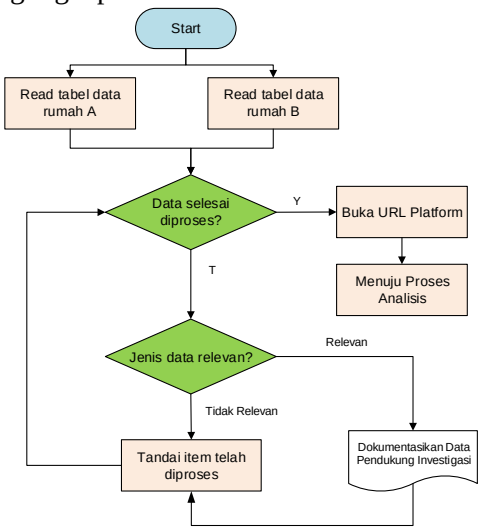
Dengan menerapkan model FAIoT [4], metode akuisisi yang digunakan untuk

mengambil barang bukti digital adalah dengan *live system* saat sistem sedang berjalan. Dalam menjalankan proses akuisisi ini tanpa mematikan atau melakukan shutdown sistem rumah cerdas.

Ancaman data terkontaminasi tidak akan terjadi dengan model FAIoT, karena log data diambil pada saat sistem berjalan namun bersumber dari server platform FAIoT bukan dari platform IoT. Sehingga pengambilan data berupa barang bukti digital tidak mempengaruhi perangkat IoT.

2. Tahap Pemeriksaan (*Examination*)

Pada tahap ini investigator forensik memeriksa hasil akuisisi barang bukti digital hasil import dari *platform* FAIoT perangkat IoT. Proses pemeriksaan akan melakukan pembacaan data dari tabel di database FAIoT Hunt dan ekstraksi data-data tersebut. FAIoT Hunt yang dikembangkan pada penelitian ini dapat melakukan klasifikasi jenis aktifitas yang dialami oleh perangkat IoT. Dengan memeriksa barang bukti digital ini investigator forensik akan mengeksplorasi data-data yang mencurigakan sebagai data pendukung dalam mengungkap kasus.



Gambar 9. Proses Pemeriksaan Barang Bukti

3. Tahap Analisis (*Analysis*)

Pada tahap ini investigasi telah melewati tahap pemeriksaan yang dilanjutkan analisis untuk mencari barang bukti digital yang terkait dengan kasus yang terjadi. Pemeriksaan telah dilakukan pada dua rumah cerdas yang menjalankan perangkat IoT. Dengan dilakukan pemeriksaan secara komprehensif maka dapat diketahui bukti-bukti digital dari setiap rumah cerdas tersebut. Analisis akan melakukan ekplorasi sistem secara mendalam untuk mencari kemungkinan-kemungkinan adanya tindakan ilegal pada sistem.

Analisis Barang Bukti Digital Rumah Cerdas A

Rumah cerdas A merupakan rumah cerdas yang dibangun berbasis perangkat IoT. Rumah cerdas A telah dilengkapi dengan model FAIoT sehingga aktifitas sistem disimpan pada server FAIoT.

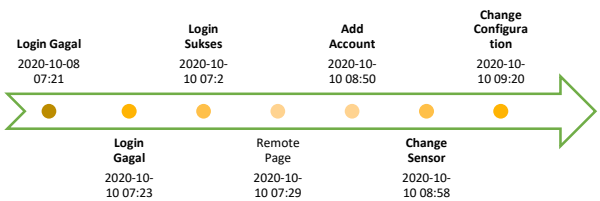
Ketika dilakukan investigasi, investigator forensik melakukan akuisisi data aktifitas sistem menggunakan aplikasi FAIoT Hunt yang juga dikembangkan dalam penelitian ini. Di bawah ini format log yang dihasilkan oleh *platform* FAIoT, terlihat bahwa log memiliki format sebagai berikut:

Gambar 3. Format log FAIoT

Dengan membaca data tersebut dapat diketahui informasi kapan terjadinya sebuah aktifitas, aktifitas apa yang dilakukan, siapa yang melakukan aktifitas.

Dari hasil analisis di dalam database FAIoT ditemukan ada dua IP Address yang mengakses sistem, yaitu IP Address 182.2.169.131 dan IP Address 117.102.64.74.

Memperhatikan aktifitas yang dilakukan IP Address tersebut pada tahap ini investigator dapat menyimpulkan bahwa pengguna dengan IP Address 117.102.64.74 telah melakukan aktifitas ilegal.



Gambar 10. *Timeline* aktifitas penyerang pada sistem IoT Rumah A

Analisis Barang Bukti Digital Rumah Cerdas B

Rumah cerdas B merupakan rumah cerdas yang dibangun berbasis perangkat IoT. Rumah

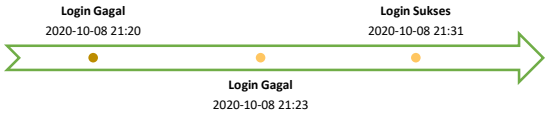
cerdas B telah dilengkapi dengan model FAIoT sama dengan rumah cerdas A sehingga aktifitas sistem disimpan pada server FAIoT.

Ketika dilakukan investigasi, investigator forensik melakukan akuisisi data aktifitas sistem menggunakan aplikasi FAIoT Hunt yang juga dikembangkan dalam penelitian ini.

Dari hasil analisis di dalam database FAIoT untuk rumah cerdas B ditemukan ada dua IP Address yang mengakses sistem, yaitu IP Address 182.2.43.155 dan IP Address 117.102.64.74.

Dari data log diungkap fakta bahwa pengguna dengan IP Address 117.102.64.74 melakukan tindakan ilegal dengan menyusup ke dalam sistem. Investigator menyimpulkan dengan tool aplikasi FAIoT pada forensik rumah cerdas B telah berhasil mendapatkan barang bukti digital.

Runtutan aktifitas Ilegal dapat digambarkan dalam timeline di bawah ini.



Gambar 11. *Timeline* aktifitas penyerang pada sistem IoT Rumah B

4. Tahap Pelaporan (*Reporting*)

Berdasarkan hasil analisis dan pengamatan dari forensik perangkat IoT berupa dua rumah cerdas yang menjadi sasaran penyerang, menunjukkan bahwa aktifitas sistem disimpan dengan baik pada platform FAIoT yang dibangun pada penelitian ini. Dengan *platform* FAIoT memudahkan investigator forensik untuk melakukan pengumpulan barang bukti digital dan menemukan fakta ketika terjadi tindakan kejahatan yang melibatkan perangkat IoT.

Hasil analisis membuktikan bahwa serangan terhadap perangkat IoT berupa dua rumah cerdas yang terdaftar di *platform* IoT berbasis Web dapat diungkap fakta kasusnya berdasarkan temuan-temuan yang dijadikan barang bukti digital.

4. KESIMPULAN

4.1 Kesimpulan

Dari hasil penelitian yang telah dilakukan dapat ditarik kesimpulan, yaitu :

1. Berdasarkan hasil analisis dan pengamatan dari forensik perangkat IoT berupa dua rumah cerdas yang menjadi sasaran penyerang, menunjukkan bahwa aktifitas sistem disimpan dengan baik pada *platform* FAIoT.
2. Hasil analisis membuktikan bahwa serangan terhadap perangkat IoT berupa dua rumah cerdas dapat diungkap fakta kasusnya berdasarkan temuan-temuan yang dijadikan barang bukti digital.

4.2 Saran

Dapat dilakukan penelitian lanjutan menggunakan analisis model forensik lain yang lebih komprehensif dan dapat dilanjutkan dengan membandingkan hasil forensik antara analisis model forensik satu dengan lainnya.

DAFTAR PUSTAKA

[1] K. K. Patel and S. M. Patel, “Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges,” *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 6122–6131, 2016.

[2] U. M. Ganesh and R. A. Khan, “Raspberry Pi Home Automation Based on Internet of Things (IoT),” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 12, pp. 301–304, 2015.

[3] R. Rizal, I. Riadi, and Y. Prayudi, “Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 382–390, 2018.

[4] S. Zawoad and R. Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” *Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015*, pp. 279–284, 2015.

[5] E. Haryanto and I. Riadi, “Forensik Internet Of Things pada Device Level berbasis Embedded System,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 6, p. 703, 2019.

[6] F. Albanna and I. Riadi, “Forensic Analysis of Frozen Hard Drive Using Static Forensics Method,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 1, pp. 173–178, 2017.