Jurnal Komtika (Komputasi dan Informatika),
Vol. 5 No. 2 | Nov 2021

Pengembangan Sistem Pemantauan dan Deteksi Serangan pada Ekosistem Rumah Cerdas

Dedy Hariyadi[1*], Chanief Budi Setiawan[2], Barep Setiyadi[3]
[1,2]Program Studi Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta
[3]Teknik Informatika Universitas Amikom Yogyakarta
*email: dedy@unjaya.ac.id

DOI: https://doi.org/10.31603/komtika.v5i2.5861

Received: 16-9- 2021, Revised: 23-10- 2021, Accepted: 26-10-2021

ABSTRACT

It is predicted that the growth of smart devices installed in the smart home ecosystem will increase in the future. Smart devices that are connected to each other using wired or wireless networks that have the potential for security holes are attacked by threat actors. Whereas a house is a place that provides comfort for its residents. An attack on the smart home ecosystem allows the operation of the smart home ecosystem to be disrupted or personal information stolen to be used by irresponsible parties. To face the high wave of smart home implementation in the future with potential security holes thatalways accompany it. This is in line with the principle that no system is 100% secure. This research shows that attacks on wireless networks can be detected as anomalous traffic. The monitoring and detection system in the smart home ecosystem involves supporting components such as sensors, access points, gateways, collectors, and analysis stacks.
Keywords: *Smart Home, Threat Actor, Wireless, Security, IDS.*

ABSTRAK

Diprediksi pertumbuhan perangkat cerdas yang terpasang pada ekosistem rumah cerdas akan meningkat pada masa yang akan datang. Perangkat cerdas yang saling terhubung menggunakan jaringan kabel maupun nirkabel yang mempunyai potensi celah keamanan diserang oleh threat actor. Padahal sebuah rumah merupakan tempat yang memberikan kenyamanan bagi penghuninya. Adanya serangan pada ekosistem rumah cerdas memungkinkan terganggunya operasional ekosistem rumah cerdas ataupun informasi pribadi yang tercuri untuk dimanfaatkan oleh pihak yang tidak bertanggung jawab. Untuk menghadapi gelombang tinggi implementasi rumah cerdas di masa akan datang dengan potensi celah keamanan yang selalu mengiringinya. Hal ini selaras dengan prinsip bahwa tidak ada sebuah sistem yang aman 100%. Pada penelitian ini menunjukan bahwa serangan pada jaringan nirkabel dapat terdeteksi sebagai lalu lintas yang anomali. Sistem pemantau dan deteksi pada ekosistem rumah cerdas melibatkan komponen pendukung seperti sensor, access point, gateway, collector, dan analysis stack.
Keywords: *Smart Home, Threat Actor, Wireless, Security, IDS.*

PENDAHULUAN

Gartner memprediksi pada tahun 2023 perangkat pintar akan meningkat kurang lebih 20 kali lipat lebih banyak [1]. Lembaga PricewaterhouseCoopers (PwC) melakukan survei perangkat pintar terbanyak yang terpasang di rumah diantaranya lampu 65%, cctv 58%, pengaman pintu 56%, pintu garasi 29%, perangkat dapur 20%, dan mobil 10% [2]. Artinya di masa akan datang di sebuah tidak hanya berisi komputer dan ponsel pintar saja melainkan rumah akan berisi perangkat pintar. Maka dapat disimpulkan bahwa definisi sebuah rumah cerdas atau smarthome adalah sebuah rumah yang terpasang sebuah perangkat pintar yang saling terhubung satu sama lain serta terpantau secara terpusat.

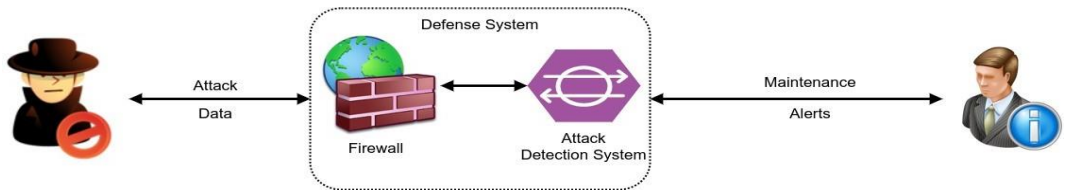
Rumah cerdas dengan perangkat cerdas yang saling terhubung memiliki potensi kelemahan keamanan informasi. Pada umumnya serangan terhadap keamanan informasi terbagi menjadi dua kategori, yaitu serangan aktif dan pasif. Sebagai bahan pertimbangan dalam keamanan rumah cerdas perlu memperhatikan empat konsep dasar, yaitu [3]:

1. *Asset*, suatu hal yang memiliki nilai untuk dilindungi.
2. *Threat*, suatu aktivitas yang memiliki potensi menyebabkan kerusakan dan kehilangan pada *Asset*.
3. *Vulnerability*, celah keamanan dalam perlindungan *Asset* dari sebuah *Threat*.
4. *Risk*, potensi dari kehilangan, kerusakan atau konsekuensi buruk sebab akibat celah keamanan.

Secara umum topologi rumah cerdas menggunakan media komunikasi jaringan nirkabel antara mesin pengendali dan sensor yang terpasang. Jaringan nirkabel yang digunakan adalah gelombang radio dengan jangkau pendek dan menengah. Adapun frekuensi radio yang digunakan diantaranya, wi-fi, bluetooth, *bluetooth low energy*, zigbee, dan z-wave. Pada frekuensi tersebut penyerang memiliki beberapa motif penyerangan, seperti [4]:

1. *Reconnaissance*, penyerang mengumpulkan informasi dari implementasi rumah cerdas untuk melakukan serangan berbahaya lainnya.
2. *Denial-of-Service (DoS)*, penyerang melakukan serangan untuk menghentikan operasional rumah cerdas.
3. *Malicious Control*, penyerang mendapatkan kendali secara tidak sah pada rumah cerdas.
4. *Device Hijacking*, penyerang membajak koneksi antara mesin kendali dan sensor atau perangkat cerdas untuk mengambil alih secara penuh rumah cerdas.

Peneliti dari perusahaan Signify N.V (sebelumnya bernama Philips Lighting N.V.), menyampaikan dalam penelitiannya bahwa jaringan nirkabel rentan diserang oleh *threatactor*. Pada penelitian yang sebelumnya obyek yang diteliti adalah protokol komunikasi Zigbee dengan potensi celah keamanan *Denial of Service* dan *Replay Attack* [4]. Sehubungan pengguna rumah cerdas di masa akan datang akan semakin banyak, potensi celah keamanan juga mengancam, dan berbagai motif penyerang rumah cerdas maka diperlukan solusi untuk mendeteksi serangan pada ekosistem rumah cerdas. Secara umum sistem deteksi pada sebuah jaringan seperti pada Gambar 1, seorang penyerang melakukan serangan ke dalam sistem pertahanan dan seorang administrator dapat memantau aktivitas penyerang [4] [5]. Oleh sebab itu pada ekosistem rumah cerdas diperlukan sebuah sistem deteksi terhadap aktivitas yang dilakukan oleh penyerang. Sehingga pemiliki rumah akan mendapatkan notifikasi jika terjadi serasa dan merasa lebih aman adanya sistem deteksi tersebut. Pada penelitian ini obyek penelitiannya pada protokol komunikasi gelombang radio 2.4GHz.

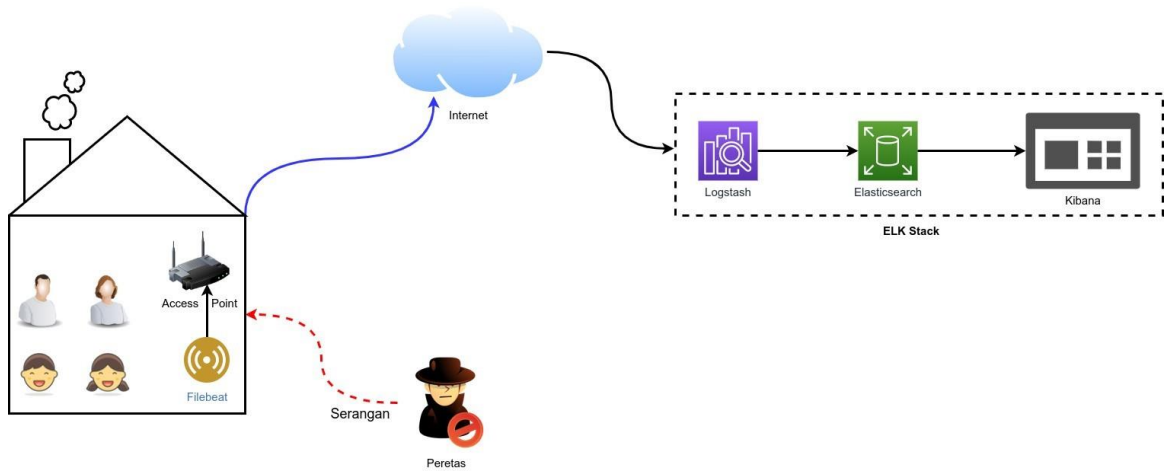


Gambar 1. Sistem Pertahanan

METODE

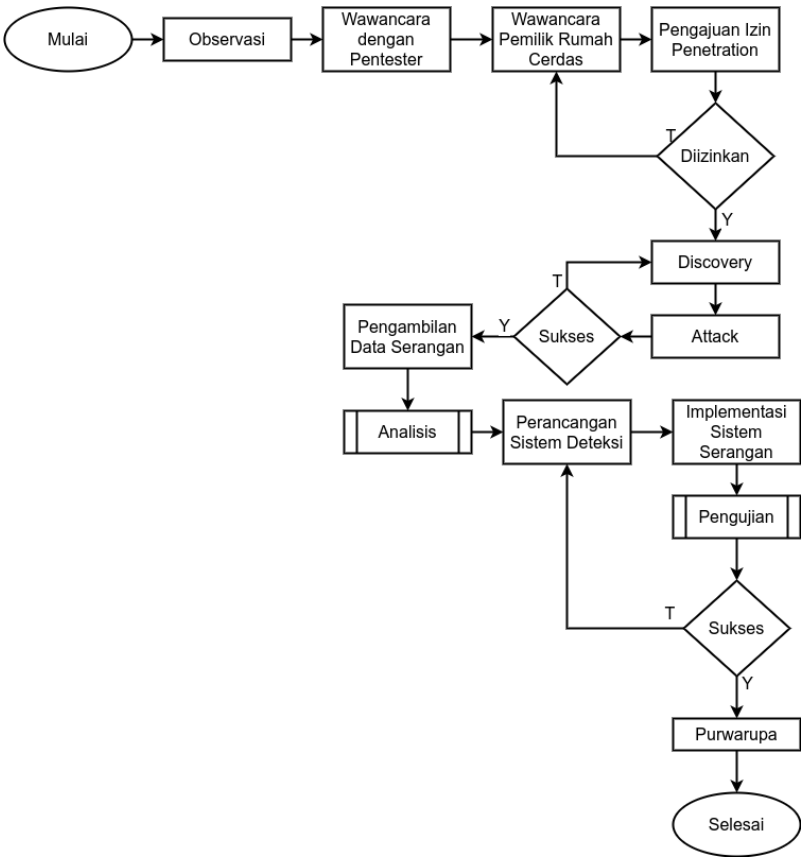
Menurut Okwori Anthony Okpe, dkk bahwa secara umum serangan terhadap ekosistem rumah cerdas diantarnya, router yang terpasang di rumah, sistem komputasi awannya, aplikasi pengendali/pemantau pada ponsel cerdas, dan keamanan fisik perangkat- perangkat cerdas. Pada ekosistem rumah cerdas perlu dipasang sistem pendeteksi yang dapat mendeteksi beberapa seranngan atau aktivitas seperti: penyalahgunaan akses, akses anomali, aktivitas perangkat cerdas yg tercatat dalam log, aktivitas perangkat cerdas melalui jaringan, dan aktivitas pada *firewall*. Catatan serangan atau aktivitas tersebut dianalisis tersebut untuk mendeteksi serangan pada berbagai macam perangkat cerdas baik tipe maupun vendor [6].

Metodologi yang digunakan oleh Praktik Satam dalam menganalisis serangan pada ekosistem rumah cerdas adalah memodelkan analisis ancaman pada protokol perangkat cerdas, mempelajari perilaku dari protokol perangkat cerdas, dan pemodelan perilaku normal untuk machine learning. Potensi serangan pada ekosistem rumah cerdas diantaranya: *deauthentication attack, disassociation attack, fake authentication attack, deauthentication broadcast attack, disassociation broadcast attack, fake power saving attack, CTS flooding attack, RTS flooding attack, probe request flooding attack, probe response flooding, man the middle attack, beacon flooding attack, modified deauthentication attack, chopchop attack, framentation attack, caffe latte attack, hirte attack, FMS attack, KoreK Family of attack, ptw attack, arp attack, dictionary attack,* dan *arp injection attack* [7]. Untuk mendeteksi serangan pada ekosistem rumah cerdas dengan infrastruktur berbasis jaringan nirkabel maka diperlukansebuah sensor yang berfungsi sebagai pengumpul data. Data yang dikumpulkan oleh sensor diolah dan disajikan menggunakan *ELK Stack* [8]. Gambar 2 menunjukan topologi yang diterapkan untuk mendeteksi serangan pada ekosistem rumah cerdas.



Gambar 2. Topologi Deteksi dan Analisis Serangan Jaringan Nirkabel

Sedangkan metode pengumpulan data pada penelitian ini menggunakan pendekatan pengujian sistem keamanan dan jaringan yang dilakukan oleh *Penetration Test* Profesional atau Pentester. Adapun pendekatan yang digunakan adalah standarisasi yang dikeluarkan oleh kementerian perdagangan Amerika Serika melalui *National Institute Standards Technologies*, yaitu NIST SP 800-42. Tahapan dasar dalam NIST SP 800-42 adalah *Planning, Discovery, Attack,* dan *Report* [9]. Gambar 3 menunjukan alur penelitian pengembangan sistem pemantauan deteksi serangan pada ekosistem rumah cerdas yang melibatkan beberapa unsur diantaranya, Pentester, pemilik rumah, dan analis keamanan siber.



Gambar 3. Alur Penelitian

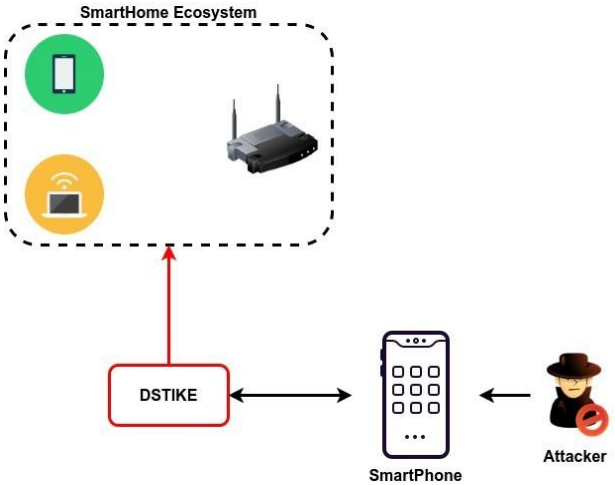
Pada penelitian ini memerlukan beberapa alat dan bahan pendukung pengujian sistem keamanan dan jaringan ekosistem rumah cerdas serta pengembangan purwarupa sistem pemantauan dan deteksi serangan. Pendekatan yang digunakan dalam penelitian adalah sistem penyerang menggunakan network penetration testing [10] dan sistem bertahan menggunakan security information and event management [11]. Oleh sebab itu diperlukan beberapa alat dan bahan pendukung seperti pada Tabel 1.

Tabel 1. Alat dan Bahan Pendukung

Alat dan Bahan	Keterangan
Deauther	DSTIKE Wi-Fi Deauther Watch DSTIKE Wi-Fi Deauther v6
Ponsel Cerdas	Xioami Poco X3 NFC
Raspberry Pi	Quad Core 1.2GHz Broadcom BCM2837 64bit CPU 1GB RAM BCM43438 wireless LAN Bluetooth Low Energy (BLE) on board 100 Base Ethernet
Kartu Jaringan Nirkabel	TP-Link TL-WN7222N
Access Point	AIoT Router, Wi-Fi 6,WPA3
Mesin Virtual	CPU 4 core, RAM 4 GB

HASIL DAN PEMBAHASAN

Proses penelitian ini menggunakan skenario serangan pada ekosistem rumah cerdas dan teknik analisis pertahanan. Tahap awal melakukan proses *discovery* menggunakan metode*war driving*, yaitu sebuah teknik untuk merekam pancaran radion jaringan nirkabel, tipe enkripsi, merk dari perangkat, dan lokasi pancaran gelombang radio menggunakan bantuan ponsel cerdas atau komputer [12]. Setelah mendapatkan informasi-informasi tersebut langkah selanjutnya melakukan serangan menggunakan *dis-authenticate* atau *deauth* pada jaringan nirkabel yang terpasang pada ekosistem rumah cerdas. Teknik ini akan mengakibatkan terputusnya koneksi pada gelombang 2.4GHz [13]. Teknik deauth menggunakan peralatan DSTIKE yang terhubung pada ponsel cerdas atau komputer. Adapun topologi serangan yang diterapkan seperti pada Gambar 5.



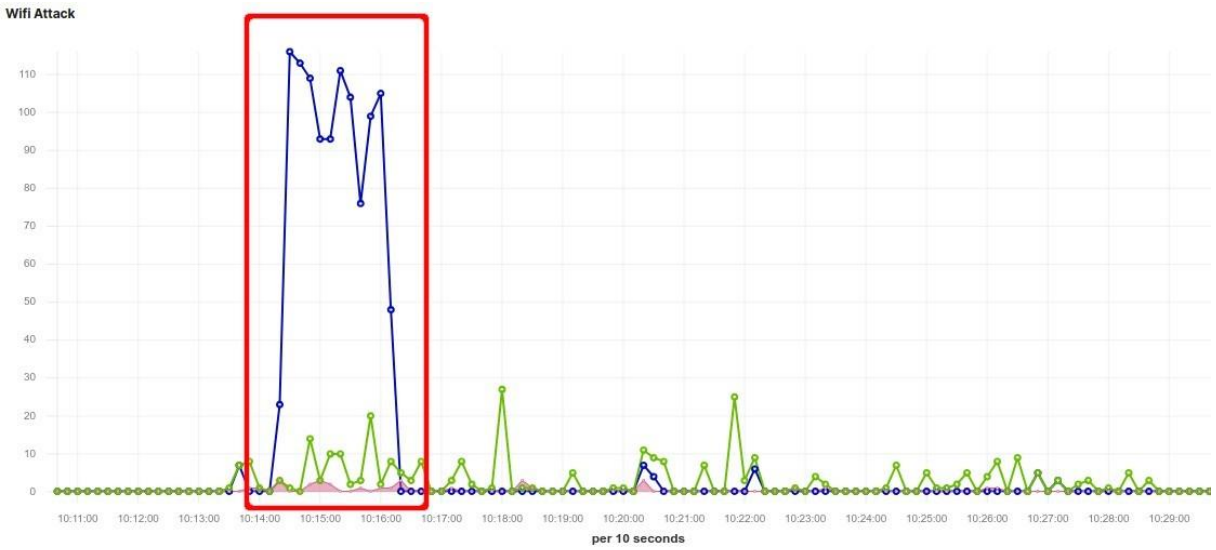
Gambar 5. Topologi Serangan

Disaat terjadi serangan *deauth* maka sensor yang telah terpasang seperti pada Gambar 2 melakukan deteksi terhadap serangan tersebut. Sensor dibangun menggunakan Raspberry dengan kartu jaringan nirkabel yang telah mendukung *Monitoring Mode*. Selanjutnya sensor melakukan perekaman aktivitas serangan yang tertangkap pada jaringan nirkabel. Dalam hal ini serangan yang dilakukan adalah *deauth*. Luaran dari rekaman tersebut disimpan dalam sebuah berkas yang selanjutnya diteruskan ke sistem pengolahan data. Cuplikan data yang tertangkap oleh sensor seperti pada Gambar 4, terlihat ada sebuah serangan ke *Routerboard* secara *broadcast* dengan *Mac Address* ff:ff:ff:ff:ff:ff dan tipe *Deauthentication*.

2021-09-09 03:14:00.940891286	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-71 dBm	QoS Data	
2021-09-09 03:14:23.748090475	00:27:22:fa:c0:a4	Ubiquiti_fa:c0:a4	b0:95:75:75:cf:a8	Tp-LinkT_75:cf:a8		1	2412 MHz	-95 dBm	Authentication	
2021-09-09 03:14:23.753959762	00:27:22:fa:c0:a4	Ubiquiti_fa:c0:a4	b0:95:75:75:cf:a8	Tp-LinkT_75:cf:a8		1	2412 MHz	-87 dBm	Authentication	
2021-09-09 03:14:28.093561194	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.131889242	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.183359502	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.252992984	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-71 dBm	Authentication	
2021-09-09 03:14:28.256520931	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-71 dBm	Association Response	
2021-09-09 03:14:28.257058011	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-71 dBm	Association Response	
2021-09-09 03:14:28.263003912	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.301952269	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-59 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.341839161	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.381961782	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.421924767	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.463133423	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.502531881	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.541805600	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.584750807	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	ff:ff:ff:ff:ff:ff	Broadcast		1	2412 MHz	-51 dBm	Deauthentication	Unspecified reason
2021-09-09 03:14:28.976313214	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-71 dBm	Association Response	
2021-09-09 03:14:28.979900327	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-69 dBm	QoS Data	
2021-09-09 03:14:28.980445116	cc:2d:e0:ea:05:98	Routerbo_ea:05:9	0c:98:38:7c:52:59	XiaomiCo_7c:52:59		1	2412 MHz	-69 dBm	QoS Data	

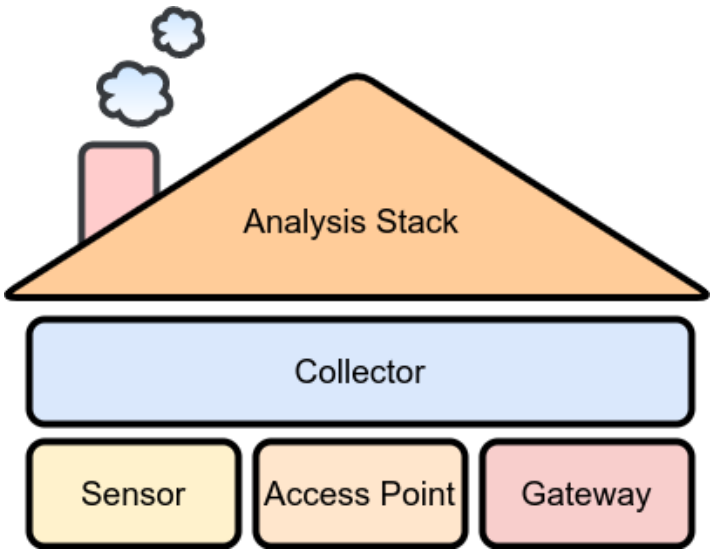
Gambar 4. Cuplikan Rekaman Serangan pada Monitoring Mode

Data rekaman tersebut diolah menggunakan *ELK Stack* untuk mempermudah pembacaan serangan sesuai skenario serangan. Data yang disajikan menggunakan *ELK Stack* dalam bentuk dashboard [14]. Pada Gambar 6 terlihat ada anomali akses jaringan nirkabel pada pukul 10.14 – 10.16. Serangan pada jaringan nirkabel dapat teridentifikasi pada *ELK Stack* saat terjadi sebuah anomali berupa lonjakan akses jaringan nirkabel.



Gambar 6. Dashboard Serangan pada *ELK Stack*

Lonjakan akses jaringan nirkabel yang terekam oleh sensor dapat dijadikan sebuah indikasi jika ada sebuah serangan jaringan nirkabel. Anomali berupa lonjakan akses jaringan nirkabel pada dapat disimpulkan telah terjadi sebuah serang pada jaringan nirkabel. Sistem pemantau seamcam ini dapat diterapkan pada ekosistem rumah cerdas maupun ekosistem yang lebih komplek untuk mendeteksi serangan *deauth*. Maka diusulkan pada sebuah ekosistem rumah cerdas perlu arsitektur seperti Gambar 7 merupakan usulan arsitektur yang dapat diterapkan yang terdiri dari lima komponen, yaitu: *Sensor, Access Point, Gateway, Collector,* dan *Analysis Stack.*



Gambar 7. Arsiterktur Sistem Deteksi Serangan Jaringan Nirkabel

KESIMPULAN

Serangan pada jaringan nirkabel dapat dimanfaatkan penyerang untuk membelokan koneksi menggunakan teknik *Man in the Middle Attack (MITM)* yang berdampak tercuri atau manipulasi data yang lewat melalui jaringan nirkabel [15]. Untuk menghindari serangan *deauthentication* yang berujung pada seranganan lanjutan menggunakan teknik MITM pada jaringan nirkabel maka pada menelitian ini mengusulkan sistem pemantauan dan deteksi menggunakan sensor yang mendukung *Monitoring Mode* dan *Analysis Stack. Monitoring mode* memungkinkan sebuah komputer dalam hal ini sensor yang mampu melakukan pemantauan lalu lintas pada jaringan nirkabel menggunakan *Wireless Network Interface Controller (WNIC)*. Dalam penelitian ini *Analysis Stack* menggunakan *Elastic-Logstash- Kibana Stack* untuk mempermudah analisis lalu lintas pada jaringan kabel sehingga dapat menyajikan lalu lintas yang bersifat anomali.

Pada penelitian ini masih memiliki kekurangan diantaranya teknik yang digunakan masih bersifat manual dalam melakukan perekaman lalu lintas pada jaringan nirkabel. Maka masih perlu perbaikan pada penelitian selanjutnya untuk ditanamkan sebuah sistem otomatisasi pada sisi sensor dan manajemen pengolahan data yang lebih kompleks. Harapannya kekurangan ini dapat diimplementasikan pada penelitian selanjutnya.

UCAPAN TERIMA KASIH

Penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia yang telah mendanai penelitian ini dan memberikan dukungan lainnya. Penelitian ini terjalin kerjasama antara Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia, Universitas Jenderal Achmad Yani Yogyakarta, dan Universitas Amikom Yogyakarta sebagai wujud program Kampus Merdeka.

DAFTAR PUSTAKA

[1] B. Burke, D. Cearley, A. Litan, D. Groombridge, und D. Mahdi, „Top 10 Strategic Technology Trends for 2020“, 2020.

[2] PwC, „Unlocking a culture of convenience“, 2017.

[3] Z. Shouran, A. Ashari, und T. Kuntoro, „Internet of Things (IoT) of Smart Home:Privacy and Security“, *Int. J. Comput. Appl.*, Bd. 182, Nr. 39, S. 3–8, 2019, doi: 10.5120/ijca2019918450.

[4] F. Sadikin und S. Kumar, „ZigBee IoT Intrusion Detection System: A Hybrid Approach with Rule-based and Machine Learning Anomaly Detection“, in *Proceedingsof the 5th International Conference on Internet of Things, Big Data and Security*, 2020,S. 57–68, doi: 10.5220/0009342200570068.

[5] S. Ul Rehman und S. Manickam, „A Study of Smart Home Environment and itsSecurity Threats“, *Int. J. Reliab. Qual. Saf. Eng.*, Bd. 23, Nr. 3, 2016, doi: 10.1142/S0218539316400052.

[6] O. A. Okpe, O. A. John, und S. Emmanuel, „Intrusion Detection in Internet of Things (Iot)“, *Int. J. Adv. Res. Comput. Sci.*, Bd. 9, Nr. 1, S. 504–509, 2018, doi: 10.26483/ijarcs.v9i1.5429.

[7] P. Satam, „A METHODOLOGY TO DESIGN INTRUSION DETECTION SYSTEMS(IDS) FOR IoT / NETWORKING PROTOCOLS“, The University of Arizona, 2020.

[8] Fazlurrahman und D. Hariyadi, „Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack“, *J. Inform. Sunan Kalijaga*, Bd. 4, Nr. 1, S. 1–8, 2019.

[9] K. Scarfone, M. Souppaya, A. Cody, und A. Orebaugh, „NIST SP 800-42: Guidelineon Network Security Testing“, Gaithersburg, MD, 2015. doi: 10.6028/NIST.SP.800-115.

[10] L. He und N. Bode, „Network Penetration Testing“, *Netw. Perim. Secur.*, 2020, doi: 10.1201/9780203508046-13.

[11] P. Cichonski, T. Millar, T. Grance, und K. Scarfone, „NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations“, 2012. doi: 10.6028/NIST.SP.800-61r2.

[12] Z. Akram, M. A. Saeed, und M. Daud, „Wardriving and its Application in Combating Terrorism“, *1st Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2018*, S. 1–5, 2018, doi: 10.1109/CAIS.2018.8442035.

[13] M. Denis, C. Zena, und T. Hayajneh, „Penetration testing: Concepts, attack methods,and defense strategies“, *2016 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2016*,2016, doi: 10.1109/LISAT.2016.7494156.

[14] J. Bullock und J. T. Parker, *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*. Indianapolis, Indiana: John Wiley & Sons, Inc., 2017.

[15] P. Anu und S. Vimala, „A Survey on Sniffing Attacks on Computer Networks“, *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, S. 1–5, 2017, doi: 10.1109/I2C2.2017.8321914.