BAB II
LANDASAN TEORI

2.1. Tinjauan Pustaka

Dalam penelitian ini, penulis akan me-*review* 5 (lima) daftar literasi yang mendukung penelitian, berdasarkan pengajuan penelitian yang akan dilakukan berikut daftar literasi yang di ambil yaitu pada **Tabel 2.1** sebagai berikut:

Tabel 2.1 Daftar Literatur

No	Penulis	Tahun	Judul Penelitian
1.	(Helmiawan. A. M. 2018)	2018	Keamanan *E-Learning* Menggunakan Metode *SQUARE* (Studi Kasus STMIK Sumedang)
2.	(Arta et al., 2021)	2021	Analisis Keamanan Informasi Aplikasi HRIS Dengan Metode *SQUARE* pada PT. XYZ
3.	(Martsanto & Nabihi, 2016)	2016	Analisis Kebutuhan Keamanan Informasi Menggunakan Metode *SQUARE* Pada Aplikasi *Remittance*
4.	(Yulianto et al., 2016)	2016	Analisis Kebutuhan Keamanan *Aplikasi E-Commerce* Dengan Menggunakan Metode Square Studi Kasus Pada Laman Web *Tokobanten.Com*
5.	(Arini et al., 2022)	2021	Uji Kerentanan Smart Home Menggunakan Metode *SQUARE* Untuk Mendukung *Smart Campus*

2.1. 1. Literatur 1

Oleh M. Agreindra Helmiawan (2018) dari Program Studi Teknik Ilmu Komputer STMIK Sumedang dengan Judul Keamanan *E-Learning* Menggunakan Metode SQUARE (Studi Kasus STMIK Sumedang). Di mana dalam penelitian yang di lakukan oleh penulis tersebut mengangkat masalah tentang melakukan analisis mengenai keamanan *E-learning*, mencegah serangan terhadap suatu *system E-learning*, dan pengendalian akses terhadap *system* tersebut. Penelitian ini menggunakan metode *SQUARE* dengan 9 (Sembilan) langkah-langkah dalam implementasi. Dalam *system E-learning* juga terdapat beberapa ancaman keamanan, hal ini di sebabkan adanya beberapa celah keamanan yang dapat di tembus oleh seorang *hacker* untuk dapat memanipulasi data sehingga keamanan *system E-learning* dapat di bajak oleh *hacker*.

Berdasarkan data hasil pengujian pada penelitian ini, dengan hal tersebut di atas, perlu di bangun suatu *system* keamanan yang dapat menjaga integritas dari *system E-learning* tersebut dengan menerapkan *system Enkripsi* dan *Deskripsi* terhadap Lalu Lintas data yang terkandung dalam *system E-Learning*. Penulis menyimpulkan dalam penelitian ini, dengan metode *SQUARE* dapat digunakan untuk menganalisis dan menguji *system* keamanan *E-Learning*, melalui metode *SQUARE* dapat di ketahui bagian yang memiliki celah keamanan yang dapat di masuki oleh pengguna berbahaya dan juga dapat di pergunakan sebagai perencanaan dalam membangun *E-Learning*, baik *system* maupun infrastruktur.

2.1. 2. Literatur 2

Oleh Yudhi Artha, Muhammad Ilhan dan Anggi Hanafiah (2021) dari Program Studi Teknik Informatika Fakultas Teknik Univesitas Riau dengan Judul Analisis Keamanan Informasi Aplikasi HRIS Dengan Metode *SQUARE* Pada PT.XYZ. Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang menjaga integritas data yang tersimpan dalam sebuah *system* maupun aplikasi. Tantangan untuk menjaga integritas data ini bermula setelah *system* terkoneksi dengan jaringan komputer yang terhubung ke internet ataupun *cloud computing* yang ada. Penelitian ini menggunakan metode *SQUARE* karena analisa kebutuhannya sangat detail sehingga rekomedasi bisa diberikan sejak tahap awal pengembangan *system* agar dapat dihasilkan sebuah *system* informasi yang lebih aman. Pada penelitian ini, penguji menggunakan 5 (lima) scenario serangan yaitu Injeksi SQL, *Data Snigging, Password Attack, Denial Of Service MAC Address Spoofing, dan Trojan*.

Berdasarkan data hasil dari pengujian pada penelitian ini, metode *SQUARE* sangat berguna untuk menganalisis dan membuat rekomendasi kebutuhan keamanan *system* yang bertujuan untuk meningkatkan ketersediaan, kontinuitas dan integritas *system* informasi HRIS PT.XYZ. metode ini memungkinkan untuk mengetahui bahwa bagian kerentanan yang dapat dimasukkan oleh pengguna jahat dan dapat digunakan sebagai perencanaan saat membangun *system* dan infrastruktur dan tidak menutup kemungkinan adanya kegagalan dalam proses analisis terutama pada bagian implementasi.

2.1. 3. Literatur 3

Oleh Sandy Martsanto dan Galih Nabihi (2016) dari Program Studi Magister Ilmu Komputer Pascasarjana Universitas Budi Luhur Jakarta Selatan Dengan Judul Analisis Kebutuhan Keamanan Informasi Menggunakan Metode *SQUARE* Pada Aplikasi *Remittance*. Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang keamanan informasi pada aplikasi *Remittance* karena aplikasi *remittance* ini rentan terhadap beberapa serangan karena berkaitan dengan transaksi uang. Sering kali persyaratan keamanan dalam rekayasa *system* dibuat berdasarkan *template* atau pola standar, tidak berdasarkan pada analisis kebutuhan sesungguhnya, di ketahui bahwa aplikasi elektronik *banking* merupakan aplikasi yang sifatnya *online* dan dapat di akses secara bebas menggunakan media internet, sama dengan mekanisme *system remittance.*

Berdasarkan data hasil dari pengujian pada penelitian ini, metode *SQUARE* menghasilkan kategorisasi dan memprioritaskan kebutuhan keamanan untuk *system*, metodologi ini terfokus membangun konsep keamanan dalam tahap awal dari siklus rekayasa *system*. Penulis dapat menyimpulkan bahwa metode *SQUARE* sangat membantu dalam menganalisis sekaligus memberikan rekomendasi terhadap kebutuhan keamanan *system* yang bertujuan untuk menjaga ketersediaan dan kontinuitas serta integritas *system remittance.*

2.1. 4. Literatur 4

Oleh Didik Yulianto, Ryan Saputra dan Rd. Ridwan Permana (2016) dari Program Pasca Sarjana Magister Komputer Universitas Budi Luhur dengan Judul Analisis Kebutuhan Keamanan Aplikasi E-*Commerce* Dengan Menggunakan

Metode *SQUARE* Study Kasus Pada Laman *Web Tokobanten.com* . Dimana dalam penelitian yang dilakukan oleh penulis mengangkat tentang masalah bagaimana menganalisis keamanan aplikasi *E-commerce* pada Laman *Web Tokobanten.com* dengan menggunakan metode *SQUARE*. Penelitian ini menggunakan metode penelitian Eksperimen dengan parameter pengujian meliputi keamanan dalam uji kecepatan responsi, Eksploit Manajemen akun, Eksploit *password* yang lemah dan Eksploit Injeksi SQL.

Berdasarkan data analisis pengujian pada penelitian ini dari tiga serangan yang dilakukan, masing-masing serangan mendapatkan hasil yang berbeda. Kemungkinan bahwa ancaman akan terwujudnya sebagai serangan nyata, dan setiap potensi konsekuensi dari serangan. Maka dari itu digunakanlah pendekatan *prototipe*. Metode ini sangat baik digunakan untuk menyelesaikan masalah kesalah pahaman antara *user* dan analis yang ditumbulkan akibat *user* tidak mampu mendefinisikan secara jelas kebutuhannya. *Prototipe* adalah pengembangan yang cepat dan pengujian terhadap model kerja dari aplikasi baru melalui proses interaksi dan berulang-ulang yang biasa digunakan ahli *system* informasi dan ahli bisnis.

2.1. 5. Literatur 5

Oleh Arin, Nurul Faizah Rozy, Lik Muhammad Malik Matin(2015) dari Jurusan Teknik Informatika Fakultas Sains Dan Teknologi UIN Syarif Hidayatullah Jakarta dengan Judul Uji Kerentanan *Smart Home* Menggunakan Metode *SQUARE* Untuk Mendukung *Smart City*. Dimana dalam penelitian yang dilakukan oleh penulis tersebut mengangkat masalah tentang bagaimana menguji kerentanan keamanan jaringan pada *smart home* yang dilakukan untuk mendapatkan hasil yang

maksimal, supaya *user* baik pemilik dapat mengetahui apa saja ancaman terhadap *smart home*.

Berdasarkan data pengujian dari penelitian ini, metode *SQUARE* berisi 9 (Sembilan) langkah untuk menangani persyaratan keamanan dan mendefinisikannya. Kerentanan pada jaringan *smart home* dapat di identifikasi. Kerentanan dapat di eksploitasi dengan menggunakan Teknik serangan DOS untuk melumpuhkan layanan *server*, *man in the middle attack* sebagai *data sniffing* dan informasi pada paket yang di transmisikan, dan *port scanning* untuk menemukan *port server* yang terbuka sebagai jalan untuk metode eksploitasi lainnya.

2.2. Jaringan Komputer

Sebuah jaringan biasanya terdiri dari dua atau lebih komputer yang saling berhubungan diantaranya satu dengan yang lainnya, dan saling berbagi sumber daya misalnya *CDROM*, *Printer*, Pertukaran File, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung tersebut dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, *satelit* atau *infrared*. Jaringan area luas (WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi *public*. WAN digunakan untuk menghubungkan jaringan area *local* yang satu dengan jaringan *local* yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi lokasi yang lain (Haryanto & Riadi, 2014)

2.3. Keamanan Jaringan

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus di lindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Komputer yang terhubung ke jaringan mengalami ancaman yang lebih besar daripada *host* yang tidak terhubung kemana-mana. Dengan mengendalikan keamanan jaringan, resiko tersebut dapat dikurangi. Namun keamanan jaringan biasanya bertentangan dengan akses jaringan, karena bila akses jaringan semakin mudah, keamanan jaringan akan semakin rawan (Rushadi, 2018).

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sering kali urutan keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang di anggap penting. Apabila menganggu performa sistem, sering kali keamanan di kurangi atau bahkan di tiadakan. Terhubungnya LAN atau komputer ke internet membuka potesi adanya mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri.

2.4. Aspek Keamanan Jaringan

Menurut (Bayu et al., 2020) dikemukakan suatu teori bahwa suatu jaringan komputer di katakan aman apabila :

2.4. 1. Privacy

Adalah sesuatu yang sifatnya rahasia atau *private*, informasi tersebut tidak dapat di akses oleh orang yang tidak di kenal atau tidak berhak. Contohnya adalah, *e-mail* atau file-file lain yang tidak boleh di baca orang lain meskipun ia adalah *administrator*.

2.4. 2. Confidentiality

Adalah data yang diberikan kepada pihak lain dengan tujuan khusus namun tetap di jaga penyebarannya. Contohnya adalah data yang bersifat pribadi seperti : Nama, Alamat, No KTP, Telepon dan lain sebagainya.

2.4. 3. Integrity

Adalah suatu informasi tidak boleh di ubah terkecuali oleh pemilik informasi tersebut. Terkadang data yang sudah terenkripsi pun tidak terjaga integritasnya karena adanya suatu kemungkinan *chaper text* dari enkripsi yang berubah. Contohnya penyerangan integritas pada saat sebuah e-*mail* di kirim di tengah jalan kemudian di sadap dan di ganti isinya, sehingga *e-mail* tersebut yang sampai ketujuan telah berubah.

2.4. 4. Authentication

ini akan di lakukan sewaktu *user login* dengan menggunakan nama *user* serta *password*-nya. Hal ini biasanya akan berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau bukan.

2.4. 5. Availability

Aspek ini berikaitan dengan apakah suatu data tersedia ketika di butuhkan atau di perlukan oleh pengguna. Jika sebuah data ataupun informasi terlalu ketat pengamanannya maka akan menyulitkan dalam akses data tersebut. Selain itu akses yang lambat juga dapat menghambat terpenuhinya aspek kebutuhannya.

2.4. 6. Non-Repudiation

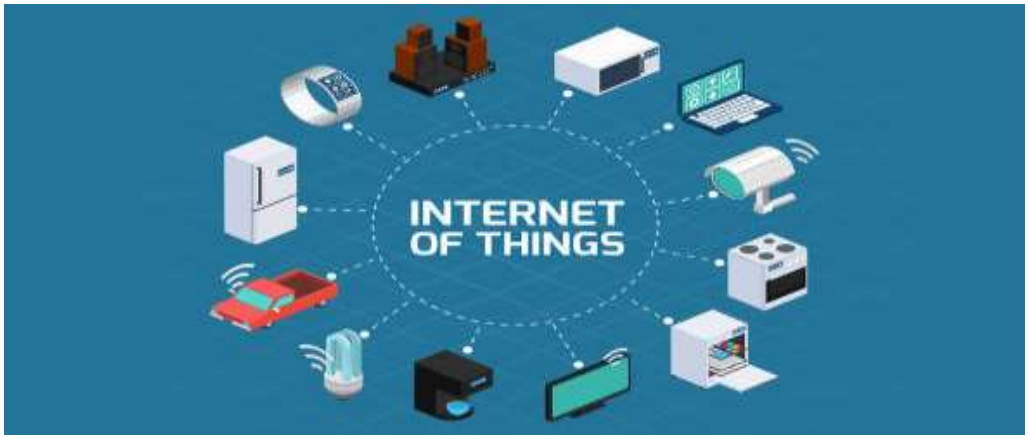
Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh seseorang mengirimkan *e-mail* untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan *e-mail* tersebut.

2.4. 7. Access Control

Dimana aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.

2.5. *Internet Of Things* (IoT)

Internet Of Thing (IoT) dapat di definisikan kemampuan berbagai *devices* yang bisa saling terhubung dan saling bertukar data melalui jaringan. IoT merupakan sebuah teknologi yang memungkinkan adanya sebuah pengendalian, komunikasi, kerjasama dengan berbagai perangkat keras, data melalui jaringan internet. Sehingga bisa di kaitkan bahwa *Internet Of Things* (IoT) adalah ketika kita menyembunyikan sesuatu *(things)* yang tidak dioperasikan oleh manusia, ke internet (Miftah, 2021).



Gambar 2.1 *Internet Of Things*

Namun IoT bukan hanya terkait dengan pengendalian perangkat melalui jarak jauh, tapi juga bagaimana berbagai data, memvirtualisasikan segala hal nyata ke dalam bentuk internet, dan lain-lain. Internet menjadikan sebuah penghubung antara sesama mesin secara otomatis. Selain itu juga adanya *user* yang bertugas sebagai pengaturan dan pengawasan bekerjanya alat tersebut secara langsung. Manfaatnya menggunakan teknologi IoT yaitu pekerjaan yang di lakukan oleh manusia menjadika lebih cepat, mudah dan efisien.

Cara kerja IoT yaitu setiap benda harus memiliki sebuah *Internet Protocol* (IP). Alamat internet *protocol* merupakan jaringan yang membuat benda bisa di perintahkan dalam sebuah identitas dari benda lain dalam jaringan yang sama. Kemudian jaringan internet tersebut akan di koneksikan ke dalam benda-benda melalui alamat internet *protocol*. Koneksi internet saat ini sudah sangat mudah di dapatkan. Setelah sebuah benda memiliki alamat IP dan terkoneksi dengan internet maka pengguna dapat memantau benda bahkan memberikan perintah *(Remote Control*) kepada benda tersebut dengan koneksi internet (Shemsi, 2018).

2.6. Smart Home

Smart home merupakan konsep rumah yang memanfaatkan teknologi baru dengan berbagai kecanggihan yang sebelumnya pernah ada. Rumah pintar ini bisa mengontrol banyak sekali aspek hunian rumah melalui *android*. Mulai dari pengaturan cahaya, fasilitas kesehatan, suhu ruangan, fasilitas hiburan, dan pengaturan lainya yang dapat mengendalikan perabotan rumah, hingga mencakup pengelolaan aspek keamanan rumah.

Smart home yang merupakan salah satu penerapan teknologi *internet of things* (IoT) dalam bidang *home automation* yang menyediakan kenyamanan, keamanan, efisiensi energi dan *control* terhadap perangkat rumah. Ada berbagai jenis area Aplikasi *smart home* seperti *smart home* untuk keamanan, *smart home* untuk orang tua, *smart home* untuk perawatan kesehatan, *smart home* untuk penitipan anak, *smart home* untuk efisiensi energi, dan *smart home* untuk hiburan, musik dan lain-lain (Arini et al., 2022).

Menurut (Mantoro et al., 2014) *Smart home* saat ini rentan dengan serangan keamanan yang meliputi :

1. ***Interruption* :** Merusak suatu perangkat *system* sehingga tidak lagi tersedia. Serangan ini mengancam kepada ketersediaan (*availability*) *system*. Contoh serangan adalah *denial of service attack.*
2. ***Interception* :** Aset atau informasi dapat di akses oleh pihak yang tidak memiliki wewenang. Contoh dari serangan ini adalah penyadapan/ *data sniffing, MAC address spoofing, dan rogue access point.*

3. ***Modification* :** selain mendapatkan akses, pihak tidak berwenang ini juga dapat mengubah (*temper*) *asset*. Contoh dari serangan ini yaitu memodifikasi isi dari *website* dengan pesan-pesan yang merugikan pemilik *website*.
4. ***Denial of service* :** serangan yang dapat menyebabkan suatu system tidak dapat melayani pihak yang sah.

2.7. SQUARE (*Security Quality Requirement Engineering*)

Security Quality Requirement Engineering (SQUARE) telah di kembangkan di *Carnegie Mel Ion University* oleh *Nancy Mead* bersama *Donald Firesmith* dan *Carol Woody* dari *Software Engineering Institute* (SEI). Proses menyediakan sarana untuk memunculkan, mengkategorikan, dan memprioritaskan persyaratan keamanan untuk *system* dan Aplikasi teknologi informasi. Tujuan jangka Panjang *SQUARE* adalah untuk mengintegrasikan pertimbangan keamanan ke dalam tahap awal siklus hidup pengembangan. *SQUARE* telah terbukti berguna untuk mendokumentasikan dan menganalisis aspek keamanan *system* lapangan dan memiliki potensi untuk mengarahkan dan memodifikasi *system* di masa mendatang ada 9 (Sembilan) tahapan menurut (Mead & Stehney, 2005).

2.7. 1. *Agree On Definition* (Mendefinisikan Kebutuhan Sistem)

Mendeskripsikan arsitektur jaringan yang akan di analisis dan mendefinisikan serta menyepakati istilah keamanan jaringan untuk *smart home* yang akan di analisis.

2.7. 2. *Identifity Security Goals* (Mengidentifikasi Tujuan Keamanan)

Menganalisis tujuan dan persyaratan keamanan sistem *internet of things* yang di perlukan oleh *smart home* untuk memastikan keamanan secara menyeluruh terhadap ketersediaan keamanan jaringan.

2.7. 3. *Develop Artifacts* (Pengembangan Artefak)

Tahap ini diperlukan apa saja artefak yang mendukung terkait dalam proses perbaikan sistem *smart home*. Artefak akan diperoleh dari kondisi yang ada pada infrastruktur di antaranya arsitektur sistem terdapat pada *smart home* yang di kembangkan sebagai perbaikan sistem, *use case*, *misuse case* dan *attack tree* yang merupakan scenario dari sistem yang ada.

2.7. 4. *Perform Risk Assessment* (Penilaian Resiko)

Hal terpenting dalam penilaian resiko ini adalah menyediakan cara yang bermakna dalam mengkategorikan keamanan jaringannya dan dampak dari ancaman utama dari sistem *smart home*-nya.

2.7. 5. *Select Elicitation Techniques* (Memilih Teknik Elisitasi)

Mengumpulkan data terkait kebutuhan apa yang akan diperlukan serta kondisi sistem secara menyeluruh dan komprehensif baik melalui metode *SQUARE,* analisa *use case* dan studi pustaka.

2.7. 6. *Elicit Security Requirements* (Permintaan Persyaratan Keamanan)

Tahap sebelumnya sudah di jelaskan bagaimana proses pengumpulan data kemudian di buat kedalam bentuk daftar kebutuhannya tentan keamanan jaringan *smart home*.

2.7. 7. *Categorize Requirement* (Kategori Kebutuhan)

Membuat daftar kategori dan rekomendasi secara detail terhadap arsitektur dan kebijakan persyaratan penerapan keamanan sistem jaringan *smart home.*

2.7. 8. *Priority Requirements* (Prioritas Kebutuhan)

Daftar prioritas dan kebijakan persyaratan penerapan keamanan sistem jaringan *smart home.*

2.7. 9. *Inspection Requirements* (Kebutuhan Penilaian)

Membuat daftar kategori dan memberikan rekomendasi detail terhadap arsitektur dan kebijakan persyaratan penerapan keamanan sistem jaringan *smart home* serta keseluruhan solusi teknis yang ada kemudian diteliti berdasarkan pada tingkatan prioritas ancaman, yang akan menyediakan semua yang di perlukan dalam rangka implementasi pada komponen inti.

2.8. Keuntungan metode *SQUARE*

Metode *SQUARE* telah terbukti menguntungkan yang mana untuk mendokumentasikan hasil dan menganalisis pekerjaan aspek keamanan jaringan, *system* yang di kerjakan berpotensi mengarahkan perbaikan dan perubahan di masa

yang akan data pada *system*. Metode ini paling efektif dan akurat bila dilakukan dengan keahlian keamanan dan pemangku kepentingan *system* keamanan jaringan. Metode *SQUARE* ini juga merupakan metode yang mencakup beberapa metode analisis keamanan jaringan. hal ini menjadikan metode *SQUARE* sebagai metode yang mampu di terapkan dalam ruang lingkup masalah yang beragam serta metode ini akan sangat diperlukan di masa yang akan datang.

2.9. Cisco Packet Tracer

Packet Tracer adalah sebuah *platform* simulasi visual alat yang di rancang oleh *cisco* sehingga memungkinkan *user* untuk membuat topologi jaringan dan meniru jaringan komputer yang lebih Modern. *Software* ini memungkinkan pengguna untuk mensimulasikan konfigurasi *cisco router* dan *switch* menggunakan simulasi antar muka baris perintah di dukung dengan sensor akuator (Miftah, 2021).

Gambar 2.2 Tampilan Awal Cisco

Packet tracer menggunakan *drag and drop user interface*, yang memungkinkan penggunanya untuk menambah serta menghapus simulasi perangkat jaringan sesuai dengan keinginan dan kebutuhan pengguna. Selain itu

juga untuk membuat simulasi dari berbagai aspek-aspek tertentu dari jaringan komputer, serta *packet tracer* juga dapat menggabungkannya (Shemsi, 2018)

Keunggulan dari *Cisco Packet Tracer* terbaru menurut (Shemsi, 2018) yaitu :

1. Menyediakan simulasi dan visualisasi mesin IoT yang praktis.
2. Mengizinkan pengguna merencanakan, membuat, menyesuaikan *smart home*, *smart garden*, dan *smart city* dengan berbagai objek pintar.
3. Menyediakan papan untuk *control* objek cerdas.
4. Mengizinkan pengguna untuk mengeksplorasi konsep prinsip-prinsip IoT.
5. Menyediakan detektor sensor.

2.10. Ancaman (*MisuseCase*)

Serangan-serangan yang sering muncul pada jaringan ini menurut (Rizkiyani, 2020) yaitu sebagai berikut:

2.10. 1. Reveal SSID

Merupakan serangan yang dilakukan dengan menyingkapkan SSID dari *access point* yang sengaja di sembunyikan oleh *administrator* jaringan komputer.

2.10. 2. DDOS

Merupakan serangan yang menyerang ketersediaan sumber daya sehingga menyebabkan *user* sah mengalami *disconnect* dari jaringan komputer.

2.10. 3. MAC *Address Spoofing*

Merupakan usaha yang dilakukan oleh seorang *hacker* untuk menembus keamanan *Mac address filtering* dengan melakukan *spoofing Mac address* pada jaringan komputer, dengan menggunakan *Mac Address user* sah untuk mendapatkan layanan jaringan komputer.

2.10. 4. Rogue Access Point

Merupakan serangan yang menggunakan suatu perangkat *Access Point* yang di buat sama dengan *Access Point* yang berada pada suatu institusi. Sehingga ketika *user* sah melakukan akses ke *Access Point* ini.

2.11. Pengertian DHCP

Dynamic Host Control Protocol atau yang di singkat dengan DHCP merupakan *protocol* internet di mana bertugas mendistribusikan segala informasi TCP/IP secara langsung kepada komputer yang terhubung dan menggunakan *protocol* TCP/IP. *Protocol* DHCP merupakan hasil perkembangan *protocol* jaringan BOOTP atau yang di kenal dengan *Bootstrap Protocol* yang memiliki kelebihan berupa alokasi otomatis ke berbagai alamat jaringan yang terhubung satu sama lain (Medianto, 2020).

DHCP berfungsi sebagai *persistent storage* atau dengan arti lain media penyimpanan menetap dari jaringan parameter untuk *client.* DHCP menyimpan sebuah *key-value* dari setiap *client* karena *key-value* ini merupakan tanda pengenal yang unik dalam tiap komputer *client* dan mengandung parameter konfigurasi

client. Tanda pengenalan unik yang terdapat dalam masing-masing komputer *client* merupakan nomor *subnet* IP (Medianto, 2020).

2.12. Penelitian Eksperimen

Eksperimen adalah sebagai suatu penelitian ilmiah dimana penelitian memanipulasi dan mengontrol satu atau lebih *variable* bebas dan melakukan pengamatan terhadap *variable-variabel* terkait untuk menemukan variasi yang muncul Bersama dengan manipulasi terhadap *variable* bebas tersebut (Setyanto, 2013).

Metode Eksperimen mengandung beberapa hal Menurut (Setyanto, 2013) sebagai berikut :

1. Suatu penelitian yang berusaha melihat hubungan sebab akibat dari satu atau lebih variable *independent* dengan satu atau lebih variable *control*.
2. Penelitian melakukan manipulasi terhadap satu atau lebih *variable independent*. Manipulasi berarti merubah secara sistematis sifat (nilai-nilai) *variable* bebas sesuai dengan tujuan penelitian.
3. Membandingkan kelompok Eksperimen yang di kenal perlakuan dengan kelompok *control* yang tidak di kenal perlakuan.
4. Pengaruh hubungan sebab akibat antara *variable* independen dengan *variable* dependen di peroleh dari selisih skor observasi masing-masing kelompok tersebut.

2.10. Metode Pengujian

Pada pengujian terdapat metode yang digunakan untuk menganalisis dan menghitung hasil dari pengujian kinerja Metode *SQUARE* yang dapat memunculkan, mengkategorikan dan memprioritaskan persyaratan keamanan untuk *system* keamanan jaringan. Tujuan jangka Panjang untuk mengintegrasikan pertimbangan keamanan ke dalam tahap awal siklus hidup pengembangan. Model ini juga dapat digunakan untuk mendokumentasikan dan menganalisis aspek keamanan *system* dalam hal perbaikan maupun improvisasi dan modifikasi *system* di masa depan. Metode inilah yang digunakan untuk mengidentifikasi kebutuhan *system*, mengidentifikasi tujuan keamanan, membangun artefak, melakukan penilaian resiko, memilih Teknik elisitasi, mendapatkan persyaratan keamanan, mengkategorikan persyaratan, melakukan prioritas persyaratan, dan kebutuhan penilaian.