BAB II

LANDASAN TEORI

2.1 Kajian Pustaka

Setelah peneliti melakukan pencarian yang relevan terhadap beberapa penelitian yang berkaitan dengan penelitian

Supriyanto (2007) dalam penelitian yang berjudul "Analisis Kelemahan Keamanan Pada Jaringan Wireless" kelemahan jaringan WiFi secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan WiFi cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor yang dapat diserang oleh hacker melalui IP spoofing [2].

Susianto, D dan Yulianti, I (2015) dalam penelitian yang berjudul "Mengamankan Wireless dengan Menggunakan Two Factor, Password dan Mac Address Filtering" menjelaskan bahwa WPA2- PSK merupakan keamanan yang menggunakan kunci enkripsi Advanced Encryption Standard (AES), yang mana AES menggunakan algoritma enkripsi canggih yang tidak bisa dikalahkan oleh alat–alat yang mengatasi keamanan TKIP yang ada pada WPA-PSK yang membuat AES menjadi metode enkripsi yang jauh lebih aman. Sudah dapat ditentukan perbedaan utama yang ada pada WPA-PSK dan WPA2-PSK yaitu

pada kunci enkripsinya, yang mana enkripsi yang digunakan pada WPA2-PSK jauh lebih aman dari enkripsi yang ada pada WPA-PSK [3].

Baihaqi, dkk (2018) dalam penelitian yang berjudul "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WI-FI" menjelaskan bahwa keamanan sistem jaringan *wireless* menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya public dan global pada dasarnya tidak aman. Adanya lubang-lubang keamanan pada sistem jaringan menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan *hacker* [4].

Zaim, S (2015) dalam penelitian yang berjudul "Apakah WPA/WPA2 Benar-Benar Aman ? Deskripsi Paket Data Terenkripsi Pada WPA/WPA2" menjelaskan bahwa yang membedakan dengan WPA adalah WPA2 menggunakan *mixed mode* yang mendukung perangkat dengan WPA dan WPA2 pada *wireless network* yang sama. Terdapat perbedaan yang signifikan antara WPA dan WPA2 yaitu WPA2 menggunakan AES untuk enkripsi data, sedangkan WPA menggunakan TKIP [5].

Iqbal, M Daulay (2019) dalam penelitian yang berjudul "Analisis Perbandingan Keamanan WEP, WPA, WPA2, Pada Access Point" menjelaskan bahwa algoritma TKIP sendiri memiliki banyak kelemahan dibandingkan AES. Sedangkan AES Enkripsi ini yang digunakan WPA/WPA2 sudah sangat kuat untuk saat ini .[1]

Fikri, A (2011) dalam penelitian yang berjudul "Analisa Perbandingan Keamanan Wireless Lan dengan Enkripsi AES (Advanced Encryption Standard) dan TKIP (Temporal Key Integrity Protocol) pada WPA" berdasarkan penelitian

yang telah di lakukan menjelaskan bahwa AES memiliki struktur yang lebih kuat dibandingkan TKIP karena tidak menyertakan data-data sensitive seperti TKIP yang dapat "ditangkap" oleh attacker, satu-satunya cara saat ini yang dapat digunakan untuk menjebol algoritma ini adalah dengan brute force. [6]

2.1.1 Tabel Perbandingan Kajian Pustaka

Nama Peneliti	Judul	Persamaan	Perbedaan
Supriyanto (2017)	Analisis Kelemahan Keamanan Pada Jaringan Wireless	Menyarankan agar melakukan penanganan terhadap kelemahan keamanan jaringan dengan cara menyembunyikan SSID, menggunakan enkripsi WEP, WPA, WPA-PSK	Tidak disertakan dengan rancangan serangan untuk membuktikan jenis keamanan tersebut dikategorikan lemah dalam mengamankan jaringan wireless
Susianto, D & Yulianti (2015)	Mengamankan Wireless dengan Menggunakan Two Factor, Password dan Mac Address Filtering	Mengamankan jaringan wireless dengan jenis keamanan WPA, menggunakan metode *Security Policy Development Life Cylce,* (SPDCL)	Tidak turut serta mencoba melakukan serangan pengujian setelah melakukan implementasi terhadap jenis keamanan yang sudah dibuat nya sebagai bukti bahwa keamanan

			yang di desain sudah benar-benar aman dari segala macam kemungkinan serangan
Baihaqi, dkk (2018)	Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi	Melakukan pengujian terhadap jenis keamanan WPA2-PSK menggunakan tools aircrack-ng sebagai alat penguji nya	tidak melakukan percobaan terhadap masing-masing algoritma yang terdapat pada jenis keamanan WPA2-PSK sehingga tidak dapat diketahui kesimpulan perbandingan diantara kedua algoritma tersebut
Zaim, S (2015)	Apakah WPA/WPA2 Benar-Benar Aman ? Deskripsi Paket Data Terenkripsi Pada WPA/WPA2	Melakukan penelitian yang memfokuskan kepada jenis keamanan WPA/WPA2 dan juga melakukan pengujian terhadap kedua jenis algoritma yang ada pada jenis keamanan WPA	Tidak memisahkan variable-variable yang di uji pada saat melakukan implementasi terkait jenis keamanan WPA/WPA2
Iqbal, M Daulay (2019)	Analisis Perbandingan	Melakukan Analisa perbandingan kemanan	Hanya melakukan Analisa perbandingan

	Keamanan WEP, WPA, WPA2, Pada Access Point	WEP, WPA, WPA2 pada acces point, menggunakan tools aircrack-ng, melakukan rancangan pengujian serangan,	pada satu jenis keamanan saja yaitu WPA
Fikri, A (2011)	Analisa Perbandingan Keamanan Wireless Lan dengan Enkripsi AES (Advanced Encryption Standard) dan TKIP (Temporal Key Integrity Protocol) pada WPA	Melakukan Analisa perbandingan algoritma TKIP dan algoritma AES pada jenis keamanan WPA	Pada penelitian ini ditambahkan sebuah rancangan pengujian terhadap algoritma TKIP dan algoritma AES menggunakan tools aircrack-ng agar mendapatkan bukti visual terhadap perbandingan kedua algoritma tersebut

Tabel 2.1 *Studie Literatur*

2.2 Dasar Teori

2.2.1 Wi-Fi

Wi-fi yang adalah satu standar *wireless networking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan [7]. Wifi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat Wireless Local Area Network (WLAN) [8]. Wifi adalah singkatan

dari Wireles Fidelity, yaitu seperangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (Wireless Local Area Network-WLAN). yang didasari pada spesifikasi IEEE 802.11 [9].

Ditinjau secara umum Wifi merupakan singkatan dari Wireless Fidelity, yang memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks - WLAN) yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.16 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya. [3]

Seperti yang sudah disampaikan di atas bahwa wifi terdiri dari beberapa variasi dalam menjalankan jaringan internet. Berikut ini adalah spesifikasi serta tingkatan kecepatan jaringan wifi tersebut.

2.2.2 Spesifikasi Wi-fi

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, yaitu:

a. 802.11a

   Sudah bekerja pada frekuensi 5 GHz dengan kecepatan transfer datanya mencapai 58 Mbps.

b. 802.11b

   Masih menggunakan frekuensi 2,4 GHz dengan kecepatan transfer datanya mencapai 11 Mbps dan jangkauan sinyal sampai 30 meter diluar ruangan.

c. 802.11g

Merupakan gabungan dari standar 802.11a dan 802.11b yang menggunakan frekuensi 2,4 GHz. Namun kecepatan akses datanya hanya mencapai 54 Mbps. Standar inilah yang umum digunakan di pasaran.

d. 802.11n

Sebagian buku menyebutnya sebagai standar masa depan yang bekerja pada frekuensi 2,4 GHz dan dikabarkan kecepatan transfer datanya dapat mencapai 100-200 Mbps [8].

Di Indonesia sendiri menggunakan spesifikasi b dengan kecepatan 11mb/s dan frekuensi band nya ~2.4Ghz. berikut adalah tampilan tabel **2.1** dari spesifikasi wi-fi

spesifikasi	Kecepatan	frekuensi band	Cocok dengan
802.11b	11 Mb/s	~2.4 Ghz	b
802.11a	54 Mb/s	~5 Ghz	a
802.11g	54 Mb/s	~2.4 Ghz	b, g
802.11n	100 Mb/s	~2.4 Ghz	b, g, n

Tabel 2.2 *Spesifikasi Wi-fi*

2.2.3 Jenis Keamanan Wi-fi

Untuk melidungi sandi wi-fi dari para peretas (*hacker*) perlu ada nya proteksi keamanan yang optimal dalam penggunaan nya. Di dalam jaringan wi-fi sendiri sudah tersedia keamanan jaringan dan dapat dipilih sesuai dengan kebutuhan nya. Ada 3 jenis keamanan wi-fi yaitu WEP, WPA, WPA2 Namun di

setiap jenis keamanan wi-fi tersebut terdapat kelebihan dan kekurangan nya masing-masing. Seperti yang ada pada Gambar **2.2** dibawah ini.

Gambar 2.1 *Jenis keamanan wi-fi*

Sumber : https://www.murdockcruz.com/2017/12/29/pilihan-wi-fi-security-mana-yang-paling-aman-untuk-kita

2.3 WPA (Wireless Protected Acces)

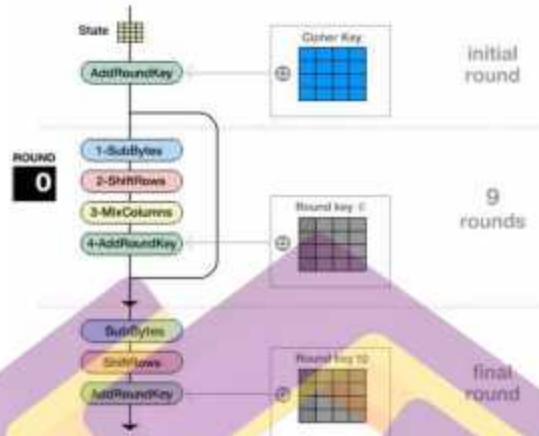
Wireless Protected Access adalah suatu sistem keamanan yang ada di dalam router. Tugas dari WPA ini adalah mengamankan jaringan nirkabel dari berbagai ancaman-ancaman yang mungkin saja terjadi. WPA ini diciptakan untuk melengkapi dari sistem pendahulu nya yaitu WEP. Diciptakan nya WPA ini adalah dikarenakan adanya celah kelemahan pada infrastruktur nirkabel yang menggunakan jenis pengaman WEP ini. WPA mengimplementasikan layer IEEE yaitu Layer 802.11i . WPA di desain untuk menggantikan metode keamanan WEP, yang menggunakan kunci keamanan static, WPA menggunakan metode TKIP (Temporal Key Integrity Protocol) yang mampu berubah secara dinamis [11]. Dalam melakukan konfigurasi untuk mengatur jenis keamanan WPA diperlukan alat tambahan berupa komper.

Fungsi dari komputer ini kemudian dikenal dengan istilah *authentication server* yang memberikan key berbeda kepada masing-masing pengguna/*client* dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Administrator dapat memilih dari dua algoritma WPA yang di sediakan, yang terdiri dari algoritma TKIP dan AES.

2.3.1 AES (Advance Encryption System)

National Institute of standards and technology (NIST) mengangkat Rijndael sebagai algoritma yang disetujui sebagai Advanced Encryption Standard (AES). AES atau rinjdael merupakan jenis enkripsi simetris blok dimana kunci pengirim dan penerima simetris. AES memiliki tiga ukuran panjang kunci yaitu 128, 192 dan 256 bit. Blok cipher Rjndael di desain seluruhnya hanya menggunakan operasi byte yang sederhana. Masing masing jenis AES mempunyai variable number of rounds. Tidak termasuk round tambahan yang diperlikan di akhir enchiperment, jumlah round dalam AES adalah sebagai berikut [12] :

1) 9 jika panjang kuncinya 128 bit
2) 11 jika panjang kuncinya 192 bit
3) 13 jika panjang kuncinya 256 bit



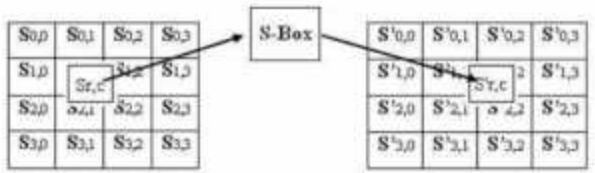
Gambar 2.2 *Enkripsi AES*

Transformasi rijndael terdiri dari 4 proses :

1. **Sub bytes**

Gambar 2.3 *Sub bytes*

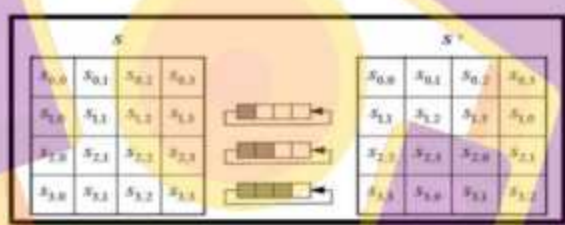
Untuk setiap byte pada array state, misalkan S[r, c] = xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S_[r, c], adalah elemen di dalam table subtitusi yang merupakan perpotongan baris x dengan kolom y. Gambar diatas mengilustrasikan pengaruh pemetaan byte pada setiap byte dalam state



Gambar 2.4 *Proses sub bytes*

2. Shiftrows

Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit). Proses pergeseran Shiftrow ditunjukkan pada **Gambar 2.6** dibawah ini :



Gambar 2.5 *Proses shift rows*

3. Mixcolumns

Transformasi Mixcolumns dilakukan setelah transformasi Shiftrows, merupakan sumber utama dari difusi pada algoritma AES, difusi merupakan prinsip yang menyebarkan pengaruh satu bit plaintext atau kunci ke sebanyak mungkin chipertext.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,0 & S1,1 & S1,2 & S1,3 \\ S2,0 & S2,1 & S2,2 & S2,3 \\ S3,0 & S3,1 & S3,2 & S3,3 \end{bmatrix} =$$

$$\begin{bmatrix} S'0,0 & S'0,1 & S'0,2 & S'0,3 \\ S'1,0 & S'1,1 & S'1,2 & S'1,3 \\ S'2,0 & S'2,1 & S'2,2 & S'2,3 \\ S'3,0 & S'3,1 & S'3,2 & S'3,3 \end{bmatrix}$$

Gambar 2.6 *Matriks Mixcolumns Transformation*

Hasil dari perkalian gambar matriks diatas tersebut, untuk setiap byte dari dalam kolom array state akan digantikan dengan nilai baru.

Gambar 2.7 *Transformasi mixcolumns*

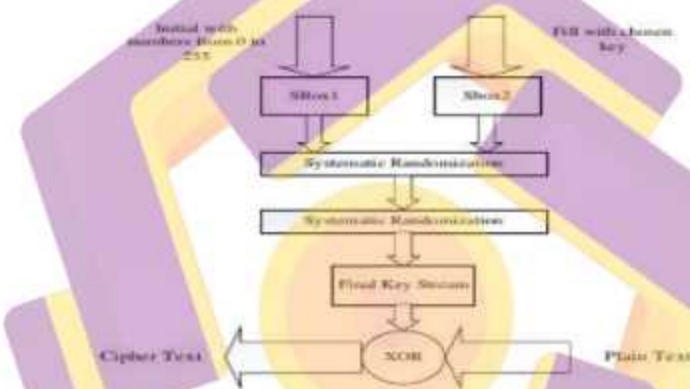
4. Add round key

Pada proses transformasi ini dilakukan operasi XOR sederhana terhadap round key dengan array state. Round key diperoleh dari cipher key sesuai nilai key masing masing round. Hasil operasi ini disimpan dalam array state.

2.3.2 TKIP (Temporal Key Integrity Protocol)

Tkip adalah algoritma yang bekerja sebagai "wrapper" untuk WEP, TKIP menggunakan pemrograman WEP asli tapi "membungkus" kode tambahan pada

bagian awal dan akhir untuk merangkum dan memodifikasi nya. Seperti WEP, TKIP menggunakan algoritma enkripsi Rivest Code 4 (RC4) streaming chipher yang mengenkripsi plaintext dengan menggunakan dua buah S-box yaitu array sepanjang 256 yang berisi permutasi dari bilangan) sampai 255 dan S-box kedia yang berisi permutasi merupakan fungsi dari kunci sebagai dasaran nya. Seperti pada gambar **2.10** dibawah ini [11] :



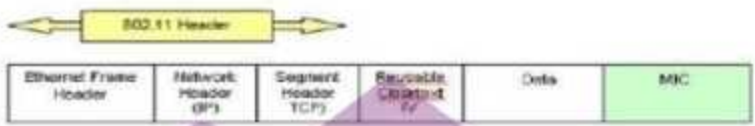
Gambar 2.8 *Metode enkripsi RC4*

Protocol baru untuk mengenkripsi setiap paket data dengan kunci enkripsi yang unik dan tombol pre-shared key yang jauh lebih kuat dibandingkan pendahulunya WEP maka untuk meningkatkan kekuatan kunci, TKIP mencakup 4 (empat) algoritma tambahan, yaitu :

1. **Message Integrity Code (MIC)**

   Mic adalah kode integritas pesan kriptografi digunakan khusus untuk memberikan integritas data untuk menjaga paket dari perubahan yang tidak sah. MIC adalah jenis kode otentifikasi pesan digunakan untuk mendeteksi

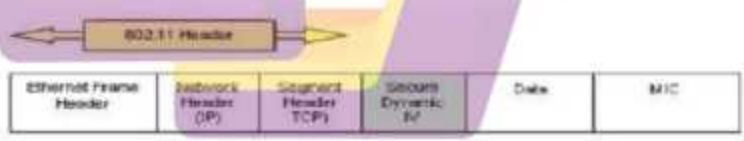
pemalsuan paket. Pada **Gambar 2.9** menunjukkan *MIC pada algoritma TKIP.*



Gambar 2.9 *MIC pada algoritma TKIP*

2. Dynamic Intialization Vector

Ada satu jenis terhadap man-in-the-middle attack yang tidak dapat di lindungi MIC. Sebuah serangan perubahan paket yang dapat terjadi Ketika pengguna yang tidak sah memperoleh paket pada pertengahan jalan (menggunakan sniffer atau protocol analyzer) dan mentransmisikan kembali setelah mengartikan informasi atau mengubah nya untuk mengurangi masalah paket perubahan ini ditambahkan vector inisialisasi, yaitu dengan menandai titik awal dari urutan enkripsi. Pada Gambar 2.11 menunjukkan DIV pada algoritma TKIP.



Gambar 2.10 *DIV pada algoritma TKIP*

3. Key scrambling and fragmentation

Pada awal proses enkripsi, TKIP menggabungkan kunci interim dengan urutan paket counter untuk membuat kunci baru kepada setiap paket nya dengan menempatkan perlindungan lain terhadap penggunaan ulang kunci.

Kemudian kunci di fragmentasikan dan setiap fragmen diberikan sebuah nomor urut. Nomor urutan fragmen kemudian digabungkan dengan kunci sementara untuk mencitakan vector inisialisasi terenkripsi untuk RC4. Pada Gambar 2.12 menunjukkan *Key mixing pada algoritma TKIP*.

Gambar 2.11 *Key mixing pada algoritma TKIP*

4. **Mekanisme re-keying untuk memberikan pembangkitan kunci setiap 10.000 paket**

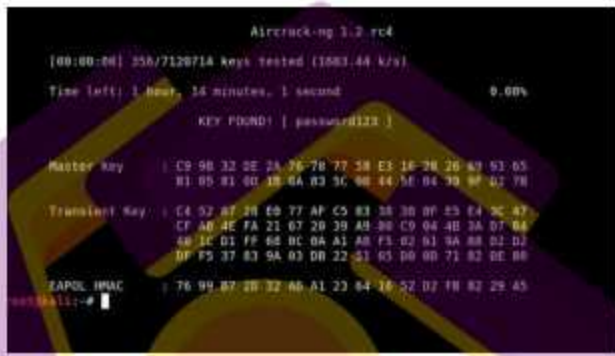
2.4 AIRCRACK

Aircrack-ng adalah suatu program yang terdapat di sistem operasi kali linux yang memiliki fungsi melakukan penetrasi / *cracking* yang berguna untuk menilai dan mengukur tingkat keamanan pada jaringan Wi-fi. Aircrack dapat bekerja pada jaringan Wi-fi dengan trafik dari 802.11a, 802.11b, dan 802.11g. [1]

2.4.1 FUNGSI AIRCRACK

1. Pemantauan : Packet capture dan ekspor data ke file teks untuk di proses lebih lanjut oleh aplikasi pihak ketiga
2. Menyerang : Serangan ulang, deauthentication, membuat akses Point palsu dan melalui via injeksi paket
3. Pengujian : Memeriksa kartu wi-fi dan kemampuan driver (capture and injection)
4. Cracking : Cracking pada WEP dan WPA PSK (WPA 1 dan 2)

Pada **gambar 2.12** dibawah ini merupakan tampilan dari aircrack-ng. seperti yang dapat dilihat pada gambar dibawah, tools aircrack-ng terdapat beberapa variable seperti key tested, time left, master key, transient key, EAPOL HMAC yang tergenerate secara otomatis dari program "aircrack-ng"



Gambar 2.12 *Tampilan aircrack*

Sumber : https://windward.solutions/6n2sr/aircrack-online.html