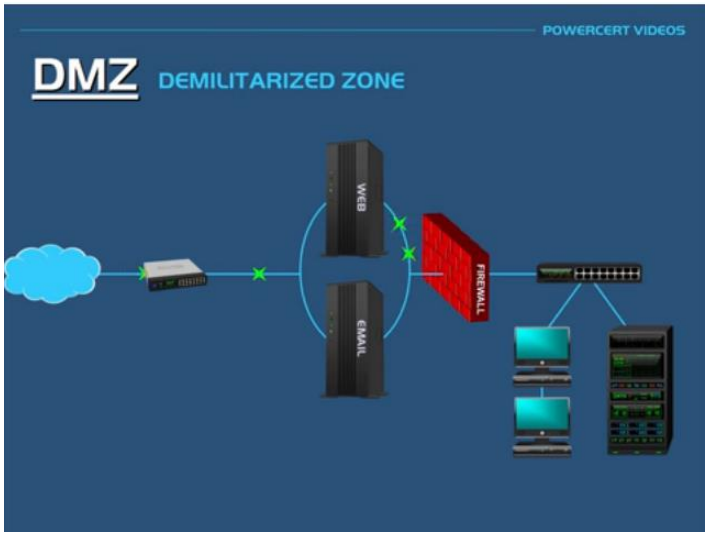
BAB II. KERANGKA TEORITIS

A. Landasan Toeri

1. Konsep Keamanan Jaringan

De-Militarized Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari gangguan hacker atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Sehingga karena DMZ dapat diakses oleh pengguna yang tidak mempunyai hak, maka DMZ tidak mengandung rules. Secara esensial, DMZ melakukan perpindahan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua port terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika hacker menyerang dan melakukan cracking pada server yang mempunyai DMZ, maka hacker tersebut hanya dapat mengakses host yang berada pada DMZ dan tidak pada jaringan internal. (Saleh Dwiyatno, Gunardi Wira Putra, Erni Krisnaningsih, 2015)

DMZ yaitu sebuah subnetwork fisik atau logis yang melindungi jaringan dalam (LAN) dari pihak luar yang tidak terpercaya. Tujuan dari DMZ adalah untuk menambahkan lapisan keamanan tambahan ke jaringan area lokal (LAN). DMZ melakukan perpindahan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua port terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika hacker menyerang dan melakukan cracking pada server yang mempunyai DMZ, maka hacker tersebut hanya dapat mengakses host yang berada pada DMZ, tidak pada jaringan internal dengan membangun *Firewall*. *Firewall* berupa perangkat lunak atau perangkat keras yang bisa menyaring paket data yang sedang melintas. *Firewall* juga bisa berupat sikap yang dibuat dan diajarkan kepada bagian IT disuatu instansi untuk merahasiakan informasi perusahan yang bertujuan untuk mencegah dan menghindari salah satu jenis hacking yaitu social enggeneering. *Firewall* juga ampuh menghambat pergerakan para penyerang yang mencoba memasuki sistem. (Gina Dayasa, Puspita Dewi, Lilik Widyawati, 2020)



Gambar 2.1. Topologi Keamanan jaringan Metode DMZ

Permasalahan pada penerapan firewall sebagai sebuah sistem keamanan jaringan komputer. Diharapkan dapat memberikan suatu pengertian tentang peranan firewall dalam mengamankan jaringan lokal terhadap kemungkinan serangan dari pihak-pihak yang tidak bertanggung jawab. Proses yang dilakukan melalui langkah-langkah yang sistematis dan ada parameter yang menjadi landasan dalam menarik kesimpulan yaitu port trafik. (Qurrotul Aini dan Victor Amrizal, 2010)

2. Ancaman

Teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari beragam ancaman atau serangan keamanan. Agar penentuan teknologi keamanan dapat sesuai dengan kebutuhan organisasi, maka diperlukan pemetaan terlebih dahulu antara jenis ancaman atau serangan dengan teknologi keamanan yang ada berdasarkan kepada aspek keamanan, yaitu: kerahasiaan (confidentiality), integritas (integrity) dan ketersediaan (availability). Firewall, IDS, antivirus system dan cryptographic system menjadi teknologi keamanan pilihan disebabkan kehandalan mereka dalam mengantisipasi dan melindungi jaringan atau sistem informasi pada aspek keamanan yang berbeda-bedaKelemahan

Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya. (Agustani Bustami, Syamsul Bahri, 2020)

B. Penelitian Rujukan

Penelitian rujukan merupakan acuan yang dibutuhkan seorang peneliti untuk melakukan penelitian. Penelitian rujukan pada penelitian ini diambil berdasarkan kesamaan permasalahan seperti Keamanan Jaringan. Banyak penelitian yang membahas tentang permasalahan tersebut dalam berbagai metode. Antara lain:

1. Thomas Setiawan (2004) menyatakan dalam penelitiannya yang berjudul **Analisis Keamanan Jaringan Internet Menggunakan *Hping, Nmap, Nessus, dan Ethereal***. Bahwa sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Penelitian tersebut hanya menganalisis keamanan jaringan Wireless tanpa adanya metode keamanan sebagai penambahan lapisan kemanaan jaringan. Berbeda dengan penelitian yang akan di kembangkan, bahwa pada objek penelitian akan menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ).
2. Aji Supriyanto (2006) menyatakan dalam penelitiannya yang berjudul **Analisis Kelemahan Keamanan Pada Jaringan *Wireless***. Bahwa pemakaian perangkat teknologi berbasis *wireless* pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi *wireless* memanfaatkan frekuensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun oleh operator yang memberikan layanan komunikasi. Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan *wireless* terbentang di atas empat *layer* di mana keempat lapis tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media *wireless*. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis *user*, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi *wireless* tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan *SSID*, memanfaatkan kunci *WEP, WPA-PSK* atau *WPA2-PSK*, implementasi fasilitas *MAC filtering*, pemasangan infrastruktur *captive portal*. Hasil penelitian tersebut hanya menganalisis keamanan jaringan Wireless dan upaya meningkatkan keamanan jaringan di penelitian tersebut

dengan menuggunakan fitur yang sudah ada di menu konfigurasi perangkat jaringan *wireless* sendiri. Berbeda dengan penelitian yang akan di kembangkan, yaitu menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ) dan lapisan keamanan di simpan dalam *server* dimana data – data sensitif tersimpan.

3. Faizin Ridho, Anton Yudhana, Imam Riadi (2006) menyatakan dalam penelitiannya yang berjudul **Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time**. Target utama *attacker* sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja router. Hal ini dapat merugikan perusahaan jasa jaringan yang bekerja sama dengan perusahaan seperti perusahaan jasa keuangan, bank, sekolah, universitas, warung internet, ataupun perusahaan *e–commerce* yang mengakibatkan transaksi berhenti. Bagi *intruder*, router sangat berperan penting untuk melancarkan aksi serangannya agar dapat masuk kedalam sistem utama atau pusat data yang diinginkan untuk melakukan tindak kejahatan. Pengendalian penuh pada router menyebabkan jaringan lain yang terhubung pada router juga dapat dikendalikan. *Intrusion Detection System* dapat dimanfaatkan sebagai sistem monitoring untuk mendeteksi serangan *distributed denial of service* (DDoS) secara *real time*. Kemampuan forensik terhadap router sangat diperlukan untuk menemukan bukti serangan yang di lakukan oleh intruder agar pelaku dapat dijerat hukum . Hasil penelitian tersebut untuk mengatasi serangan dari *attacker* yaitu dengan menambahkan Forensik Router guna menambah lapisan keamanan jaringan. Berbeda dengan penelitian yang akan di kembangkan, yaitu menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ) dan lapisan keamanan di simpan dalam *server* dimana data – data sensitif tersimpan.
4. Sonny Rumalutur (2014) menyatakan dalam penelitiannya yang berjudul **Analisis Keamanan Jaringan *Wireless LAN (WLAN)* Pada PT. PLN (Persero) Wilayah P2B Area Sorong**. Bahwa penelitian ini membahas tentang analisis keamanan *Wireless Local Area Network (Wireless LAN)* di PT. PLN (Persero) Wilayah P2B Area Sorong terhadap serangan luar pada protokol *Wireless Protected Access (WPA), Web Proxy*, dan *Virtual Private Network (VPN)*, digunakan untuk menyerang *LAN*. Tiga jenis perangkat lunak yang digunakan sebagai penyerang yaitu, penyerang *Network Stumbler*, *Aircrack* dan *Wireshark*. Perangkat lunak tersebut digunakan di laptop pada jarak 5m sampai 25m dari titik akses *LAN* Nirkabel. Dari hasil eksperimen terlihat waktu tercepat direspon oleh Protokol WPA diberikan oleh penyerang *Network Stumbler*, diikuti

oleh *Aircrack* dan *Wireshark*. Hasil penelitian diatas adalah analisis keamanan jaringan *Wireless LAN*. Perbandingan dengan penelitian yang akan dikembangakan, yaitu dengan menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ) dan lapisan keamanan di simpan dalam *server* dimana data – data sensitif tersimpan.

5. Saleh Dwiyatno, Gunardi Wira Putra, dan Erni Krisnaningsih (2015) menyatakan dalam penelitiannya yang berjudul **Penerapan *OspfRouting, De-Militarized Zone*, Dan *Firewall* Pada Mikrotik Routerboard Dinas Komunikasi Dan Informatika Depok**. Hasil dari penelitian ini adalah terbentuknya koneksi antar jaringan dalam topologi beserta suksesnya fungsi dari firewalldan bekerjanya ruleuntuk area DMZ. Keberhasilan dalam pengaplikasian diuji kembali dengan melakukan beberapa metode serangan yang akan ditanggulangi oleh konfigurasi yang telah diterapkan pada alat jaringan beserta server.
6. Daniel Hoffman dan Kevin Yoo (2005) menyatakan dalam penelitiannya yang berjudul ***Blowtorch: a framework for Firewall test automation.*** *Firewall* memainkan peran penting dalam keamanan jaringan. Pengalaman menunjukkan bahwa pengembangan set aturan *Firewall* rumit dan rentan kesalahan. Kesalahan kumpulan aturan bisa mahal, dengan membiarkan lalu lintas rusak atau dengan memblokir lalu lintas yang sah dan menyebabkan aplikasi penting gagal. Akibatnya, pengujian *Firewall* sangat penting. Sayangnya, ini juga sulit dan ada sedikit dukungan alat yang tersedia.Blowtorch adalah kerangka C ++ untuk pembuatan uji *Firewall*. Konstruk pusat adalah paket iterator: generator yang digerakkan oleh peristiwa dari aliran paket yang dicentang waktu. Blowtorch mendukung pengembangan iterator paket dengan pustaka untuk pembuatan dan penguraian header paket, penjadwal pengiriman untuk multiplexing beberapa stream paket, dan monitor penerima untuk demultiplexing aliran paket yang tiba. Kerangka kerja ini menyediakan iterator yang menghasilkan aliran paket menggunakan array yang meliputi, tata bahasa produksi, dan memutar ulang lalu lintas TCP yang ditangkap. Blowtorch telah digunakan untuk mengembangkan tes untuk *Firewall* industri yang ditempatkan antara jaringan TI dan jaringan kontrol proses. Perbandingan dengan penelitian yang akan dikembangkan bahwa firewall dibuat dan diterapkan di Linux sebagai Server untuk memisahkan dan membatasi akses diantara dua Jaringan antara jaringan *client* dan *server*. Jaringan *server* dilindungi dengan teknologi lapisan Firewall untuk melindungi *server* dari serangan – serangan jaringan.
7. Si Choon Noh, Dong Chun Lee, Kuinam J. Kim (2003) menyatakan dalam

penelitiannya yang berjudul ***Improved Structure Management of Gateway Firewall Systems for Effective Networks Security.*** Dalam tulisan ini mereka mengusulkan peningkatan manajemen struktur sistem *Firewall* gateway. Manajemen ini memiliki keamanan jaringan yang efektif dibandingkan dengan manajemen struktur umum yang terdiri dari konfigurasi jaringan, manajemen topologi, topologi dan manajemen peran host bastion, manajemen kontrol peralatan jaringan, dan beberapa *Firewall*. Hasil penelitian diatas adalah upaya untuk meminimalisir kerentanan serangan jaringan dengan menggunakan salah satu teknik pembuatan firewall yaitu, *Port Knocking*. Sedikit berbeda dengan penelitian yang akan dikembangkan bahwa teknik yang digunakan hampir sama yaitu menggunakan teknik pembuatan firewall, namun hal yang membedakan adalah firewall yang dibuat untuk menahan serangan atau memperlambat hacker itu dengan upaya memanipulasi *IP Routeable* yang bertujuan untuk memperlambat kegiatan hacker.

8. Diane Tang dan Mary Baker (2000) menyatakan dalam penelitiannya yang berjudul ***Analysis of a local-area wireless network*** (, Stanford University, 2000).Menganalisis jaringan untuk perilaku pengguna secara keseluruhan (kapan dan seberapa intensif orang menggunakan jaringan dan seberapa banyak mereka bergerak), keseluruhan lalu lintas jaringan dan karakteristik pemuatan (mengamati throughput dan simetri lalu lintas masuk dan keluar), dan karakteristik lalu lintas dari titik pengguna (campuran aplikasi yang diamati dan jumlah host yang terhubung oleh pengguna). Di antara hasil lainnya, mereka menemukan bahwa pengguna dibagi ke dalam sub-komunitas berbasis lokasi yang berbeda, masing-masing dengan gerakan, aktivitas, dan karakteristik penggunaannya sendiri. Sebagian besar pengguna mengeksploitasi jaringan untuk penjelajahan *web*, aktivitas berorientasi sesi, dan aktivitas berorientasi obrolan. Banyaknya kegiatan yang berorientasi pada obrolan menunjukkan bahwa banyak pengguna memanfaatkan jaringan seluler untuk komunikasi sinkron dengan yang lain. Selain hasil spesifik pengguna ini, mereka menemukan bahwa *throughput* puncak biasanya disebabkan oleh satu pengguna dan aplikasi. Selain itu, sementara lalu lintas masuk mendominasi lalu lintas keluar, sebaliknya cenderung benar selama periode *throughput* puncak, menyiratkan bahwa asimetri yang signifikan dalam kapasitas jaringan dapat tidak diinginkan bagi pengguna mereka. Meskipun hasil ini hanya berlaku untuk jaringan nirkabel dan komunitas pengguna area lokal ini, mereka percaya bahwa lingkungan yang serupa dapat menunjukkan perilaku dan tren yang serupa. Mereka berharap bahwa pengamatan mereka akan berkontribusi pada

pemahaman yang berkembang tentang perilaku pengguna ponsel. Perbandingan yang hampir sama dengan penelitian yang akan dikembangkan, bahwa penelitian ini diterapkan dalam jaringan area lokal. Namun yang membedakan dengan penelitian yang akan di kembangkan, yaitu menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ) lapisan keamanan jaringan yang di simpan dalam *server* dimana data – data sensitif tersimpan.

9. Matthias Schmidt, Matthew Smith, Niels Fallenbeck, Hans Picht, Bernd Freisleben (2007) menyatakan dalam penelitiannya yang berjudul ***Building a Demilitarized Zone with Data Encryption for Grid Environments***. Keamanan dan integritas data adalah aspek penting dalam bidang komputasi Grid dan cluster. Ketika kedua area ini digabungkan, masalah keamanan akan berbaur dan baru konsep keamanan diperlukan untuk memastikan perlindungan keduanya Pengguna grid dan pengguna cluster lokal. Dalam tulisan ini, sebuah novel Dual laned Demilitarized Zone (DMZ) untuk melindungi cluster lokal dari serangan Grid diperkenalkan. Keamanan Globus Infrastruktur (GSI) diperluas untuk memungkinkan ujung ke ujung yang aman enkripsi pekerjaan Grid melalui DMZ dan ke host eksekusi tervirtualisasi. Akhirnya, Sistem Deteksi Intrusi Jaringan terintegrasi dengan aturan khusus Grid, selanjutnya melindungi Grid DMZ.
10. David Kotz (2005) dan Kobby Essien (2005) menyatakan dalam penelitiannya yang berjudul ***Analysis of a Campus-Wide Wireless***. Bahwa memahami pola penggunaan dalam jaringan area lokal nirkabel (WLAN) sangat penting bagi mereka yang mengembangkan, menyebarkan, dan mengelola teknologi WLAN, serta mereka yang mengembangkan sistem dan perangkat lunak aplikasi untuk jaringan nirkabel. Makalah ini menyajikan hasil dari jejak terbesar dan paling komprehensif dari aktivitas jaringan di LAN nirkabel produksi yang besar. Selama sebelas minggu mereka menelusuri aktivitas hampir dua ribu pengguna yang diambil dari populasi kampus umum, menggunakan jaringan 476 titik akses kampus yang tersebar di 161 gedung di Dartmouth College. Studi mereka
11. memperluas yang dilakukan oleh Tang dan Baker, dengan populasi yang secara signifikan lebih besar dan lebih luas. Mereka menemukan bahwa lalu lintas perumahan mendominasi semua lalu lintas lainnya, terutama di tempat tinggal yang dihuni oleh siswa baru; siswa semakin memilih laptop nirkabel sebagai komputer utama mereka. Meskipun protokol web adalah komponen tunggal terbesar dari volume lalu lintas, cadangan jaringan dan berbagi file berkontribusi besar dalam jumlah lalu lintas. Meskipun ada beberapa roaming

dalam sesi jaringan, mereka dikejutkan oleh sejumlah situasi di mana kartu berkeliaran secara berlebihan, tidak dapat puas pada satu titik akses. Roaming lintas-subnet adalah masalah utama, karena mereka memutuskan koneksi IP, menunjukkan perlunya solusi yang menghindari atau mengakomodasi roaming semacam itu. Hasil penelitian diatas adalah analisis keamanan jaringan *Wireless LAN*. Perbandingan dengan penelitian yang akan dikembangakan, yaitu dengan menambahkan lapisan keamanan jaringan dengan menggunakan Metode *Demilitarized Zone* (DMZ) dan lapisan keamanan di simpan dalam *server* dimana data – data sensitif tersimpan.

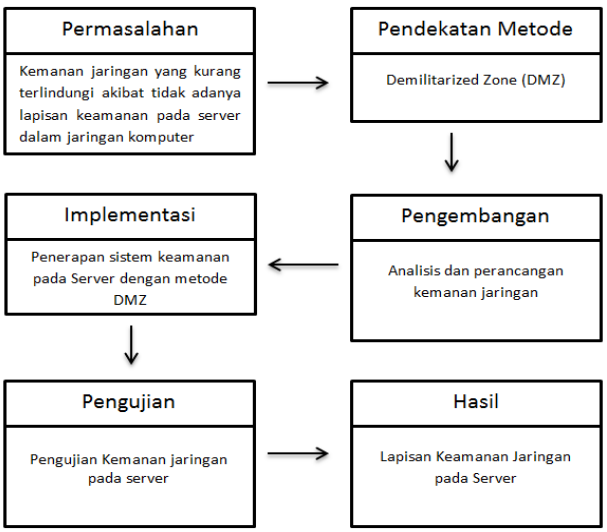
Tabel 2.1 Tabel tinjauan pustaka

No	Peneliti / tahun	Jurnal Sumber	Judul Penelitian	Kontribusi
1	Thomas Setiawan (2004)		Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal	Analisis kemaanan jaringan yang masih rentan terhadap serangan jaringan.
2	Aji Supriyanto (2006	Jurnal Teknologi Informasi DINAMIK Volume XI, No. 1, Januari 2006 : 38-46 ISSN : 0854-9524	Analisis Kelemahan Keamanan Pada Jaringan Wireless	Analisis keamanan jaringan Wireless dan upaya meningkatkan keamanan jaringan di penelitian tersebut dengan menggunakan fitur yang sudah ada di menu konfigurasi perangkat jaringan wireless sendiri.
3	Faizin Ridho, Anton Yudhana, Imam Riadi (2006)	ISBN : 979-587-626-0 | UNSRI	Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time	Intrusion Detection System dapat dimanfaatkan sebagai sistem monitoring untuk mendeteksi serangan distributed denial of service (DDoS) secara real time.
4	Sonny Romalutur (2004)	Jurnal Teknologi dan Rekayasa, Volume 19 No. 3, Desember 2014	Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong	analisis keamanan jaringan Wireless LAN
5	Saleh Dwiyatno, Gunardi Wira Putra, dan Erni Krisnaningsih (2015)	Jurnal Sistem Informasi Volume.2, 2015 ISSN: 2406-7768	Penerapan OspfRouting, De-Militarized Zone, Dan FirewallPada Mikrotik RouterboardtmDinas Komunikasi Dan InformatikaDepok	mengaplikasikan konfigurasi dari Routing, De-Militarized Zone dan Firewall pada alat jaringan MikroTik

				membuat jalur data pada jaringan memiliki kinerja yang lebih baik
6	Daniel Hoffman (2005) dan Kevin Yoo (2005)	Department of Computer Science PO Box 3055 STN CSC	Blowtorch: a framework for Firewall test automation	Menggunakan Blowtorch untuk mengembangkan tes Firewall industri yang ditempatkan antara jaringan TI dan jaringan kontrol proses
7	Si Choon Noh, Dong Chun Lee, Kuinam J. Kim (2003)	ISCIS 2003, LNCS 2869, pp. 1076–1083, 2003	Improved Structure Management of Gateway Firewall Systems for Effective Networks Security	Meminimalisir kerentanan serangan jaringan dengan menggunakan salah satu teknik pembuatan firewall yaitu, *Port Knocking*.
8	Diane Tang (2000) dan Mary Baker (2000)	Stanford, CA 94305-9030 Stanford, CA 94305-9040	Analysis of a local-area wireless network, 2000	analisis keamanan jaringan Wireless LAN
9	Matthias Schmidt, Matthew Smith, Niels Fallenbeck, Hans Picht, Dan Bernd Freisleben (2007)	Hans-Meerwein-Strasse, D-35032 Marburg, Germany Copyright 2007 ACM ICST 978-963-9799-07-3	Building a Demilitarized Zone with Data Encryption for Grid Environments	teknik Hot spot. Teknik penyamaran trafik jaringan membuat banyak area acak dari aktivitas komunikasi tinggi tujuan menghambat atau meminimalisir serangan jaringan seperti analisis trafik lalu lintas jaringan
10	DAVID KOTZ (2005) dan KOBBY ESSIEN (2005)	Wireless Networks 11, 115–133, NH 03755	Analysis of a Campus-Wide Wireless Network, 2005	analisis keamanan jaringan Wireless LAN.

C. Kerangaka Pemikiran

Berikut adalah kerangka pemikiran untuk memecahkan masalah penelitian ini yang digambarkan pada gambar berikut:



Gambar 2.2. Kerangka Pemikirian

Penjelasan tentang Kerangka Pemikiran pada penilitan ini adalah:

1. Identifikasi masalah untuk menetapkan tujuan Penelitian.

   Penambahan lapisan keamanan jaringan dengan menggunakan metode Demilitarized Zone (DMZ).
2. Melakukan pendekatan Metode *Demilitarized Zone* untuk membangun lapisan keamanan Jaringan pada Komputer *Server*.

   Penerapan metode DMZ ini disimpan pada server yang berbasis sistem oprasi *Linux ubuntu 16.04.*
3. Melakukan pengembangan melalui tiga tahap, yaitu tahap perancangan, tahap pengujian dan tahap implementasi.

   Pengembangan yang dilakukan agar kebutuhan jaringan pada server dapat meminimalisir terhadap serangan jaringan.
4. Melakukan Implementasi sistem kemanan jaringan pada server.

   Sistem keamanan yang dirancang dan dibuat sesuai yang dibutuhkan pada permasalahan.
5. Melakukan pengujian pada keamanan server.

   Pengujian yang dilakukan menggunakan tools khusus, dengan tujuan mendapatkan hasil yang cukup pada sistem keamanan jaringan pada server.
6. Mendapatkan hasil dari 3 tahap perancangan, pengujian dan impementasi pada sistem keamanan jaringan.

   Evaluasi dilakukan apabila teridentifikasi kekurangan dalam prakteknya dan mencari solusi agar kekurangan tersebut dapat teratasi.