PENGEMBANGAN APLIKASI REMOTE BERBASIS ANDROID UNTUK KONFIGURASI INTRUSION PREVENTION SYSTEM MEMANFATKAN INTERNET OF THINGS

Rinanza Zulmy Alhamri [1], Kunti Eliyen [2], Agustono Heriadi [3]
[1,2,3] Politeknik Negeri Malang, Jl. Soekarno Hatta No. 9 Kota Malang
rinanza.z.alhamri@polinema.ac.id

ABSTRAK

Router MikroTik mampu untuk dikonfigurasi sebagai Intrusion Prevention System (IPS) sehingga dapat menolak paket data yang memiliki perilaku sebagai serangan Port Scanning, Brute Force, dan Denial of Service. Dikembangkan aplikasi Android yang dapat melakukan kendali jarak jauh pada router MikroTik secara fleksibel dan efisien dengan bantuan aplikasi Agent berbasis web memanfaatkan library MikroTik API dan media penyimpanan cloud Firebase sehingga aplikasi bisa dijalankan secara Internet of Things (IoT). Terdapat enam tahapan meliputi pengumpulan data, analisis sistem, perancangan sistem, implementasi, pengujian dan pembuatan laporan. Analisis sistem menghasilkan fungsi meliputi admin dapat mengaktifkan aplikasi Agent, mengelola konfigurasi IPS Port Scanning, Brute Force, serta Denial of Service, melihat daftar IP penyerang dan memperoleh notifikasi serangan baru. Aplikasi Agent dikembangkan dengan Laravel memanfaatkan library RouterOSAPI untuk komunikasi API, vendor kreait untuk koneksi ke Firebase baik Firestore maupun Real-time Database, dan Javascript fungsi setInterval() agar aplikasi web berjalan otomatis. Sedangkan aplikasi remote Android dikembangkan dengan bahasa Kotlin menggunakan Android Studio. Berhasil dikembangkannya aplikasi remote berbasis Android untuk konfigurasi IPS dalam mencegah serangan Port Scanning, Brute Force, dan Denial of Service melalui Internet of Things. Hasil pengujian fungsional dilakukan dengan menguji aplikasi Android untuk dapat mengendalikan konfigurasi IPS secara remote oleh responden sebagai pengguna aplikasi dimana keberhasilan mencapai 91,67%. Sedangkan hasil pengujian kinerja konfigurasi IPS dilakukan dengan memberikan skenario serangan Port Scanning, Brute Force, serta Denial of Service pada router MikroTik dimana keberhasilan dalam bertahan mencapai 72.5%.

Keyword : *aplikasi android, Intrusion Prevention System, Internet of Things*

1. PENDAHULUAN

Penanganan serangan-serangan pada jaringan bisa dicegah dengan pengembangan Intrusion Prevention System (IPS). IPS merupakan sebuah sistem yang berfungsi untuk menolak paket data yang telah dicurigai sebagai suatu serangan serta memberikan peringatan adanya serangan[1]. Perangkat IPS dikonfigurasi secara implementatif untuk menolak secara langsung, paket-paket yang bersumber dari alamat yang telah dicurigai sebagai penyerang. Hal ini berbeda dengan peran Intrusion Detection System yang hanya mendeteksi sumber paket dengan menganalisa apakah sumber tersebut serangan atau bukan. Penerapan IPS efektif untuk menghadang serangan pada jaringan komputer berupa serangan Denial of Service atau serangan Brute Force dengan memberikan konfigurasi berbasis IPS pada router untuk menolak masuknya paket data yang memiliki perilaku mencurigakan.

Implementasi IPS pada router berbasis MikroTik bisa memanfaatkan fungsi dan konfigurasi yang disediakan RouterOS MikroTik. Konfigurasi IPS untuk setiap serangan memiliki konfigurasi yang berbeda. Pada hasil penelitian [2], konfigurasi IPS untuk menolak paket data yang dicurigai sebagai Brute Force dan Port Scanning bisa dilakukan dengan konfigurasi aturan pada Firewall Filter. Hasilnya Mikrotik mampu menolak serangan Brute Force dan Port Scanning dengan baik. Hal tersebut juga dipraktikkan oleh penelitian [3], di mana melakukan konfigurasi aturan Firewall Filter untuk menolak serangan Brute Force dan Port Scanning.

Sedangkan untuk mencegah serangan Denial of Service (DoS), penelitan [4] melakukan konfigurasi aturan pada Firewall Filter dan Firewall Raw. Hasilnya pengaturan konfigurasi Firewall Filter dan Firewall Raw terbukti efektif mencegah terjadinya peningkatan kinerja resource akibat serangan DoS. Untuk bahan analisis dilakukan pencatatan aktivitas percobaan DoS dengan Firewall Log. Begitupula pada penelitian [5], dengan melakukan konfigurasi pada Firewall Raw, router MikroTik mampu menahan serangan DoS jenis Syn Flood sehingga resource router aman dari terjadinya kondisi *down*.

Dengan fungsi router MikroTik untuk menolak serangan Brute Force, Port Scanning, dan Denial of Service melalui konfigurasi Firewall membuat administrator memang perlu untuk menerapkan konfigurasi keamanan jaringan [6]. Pada kondisi *existing*, konfigurasi router oleh admin dilakukan secara *on-site*. Padahal dengan perkembangan teknologi Internet of Things (IoT), memungkinkan sistem dapat dikendalikan dari jarak jauh melalui internet sehingga tujuan konfigurasi kemanan pada

router bisa dilakukan [7]. Diperlukan sebuah aplikasi yang mampu melakukan kontrol router secara remote sehingga konfigurasi IPS pada router MikroTik bisa dilakukan dimanapun dan kapanpun.

Sebelumnya, telah banyak penelitian yang mengembangkan aplikasi kendali jarak jauh untuk mengendalikan router. Penelitian [8] telah mengembangkan aplikasi Android untuk mengelola bandwidth pada traffic pada jaringan berbasis MikroTik. Sedangkan pada penelitian [9] juga mengembangkan aplikasi Android memanfaat MikroTik Applicaion Programming Interface (API) untuk mengelola bandwidth pada traffic jaringan. Kemudian pada penelitian [10] mengenalkan konsep IoT dalam mengendalikan router berbasis Software Defined Network (SDN) menggunakan sistem operasi OpenFlow, sehingga jaringan berbasis AWG-STAR bisa dikendalikan secara lebih fleksibel. Hal ini membuktikan bahwa teknologi IoT dapat dimanfaatkan sebagai perantara pengendali jarak jauh dalam mengendalikan suatu sistem khususya router berbasis MikroTik.

Dari berbagai penelitian yang telah dilakukan sebelumnya, pengembangan aplikasi pengendali jarak jauh pada router masih menitikberatkan pada fungsi umum dari jaringan seperti monitoring dan load balancing. Belum ada penelitian yang membahas khusus untuk implementasi keamanan jaringan dengan aplikasi remote berbasis Android. Saat ini sistem operasi Android mengalami peningkatan penggunaan yang sangat pesat. Daripada menggunakan aplikasi berbasis web, aplikasi berbasis Android lebih unggul terutama pada kecepatan, keamanan, serta lebih mudah untuk dikembangkan dengan adanya berbagai macam *tools.* Meskipun jumlah aplikasi Android masih jauh lebih kecil dibandingkan aplikasi website, namun pengguna aplikasi Android mengalami peningkatan yang lebih signifikan dibandingkan aplikasi website di PC maupun di perangkat mobile. Sehingga dengan aplikasi yang dapat berjalan pada Android, selain penggunaan yang lebih fleksibel, juga lebih handal dengan dukungan teknologi yang masih berkembang.

Pada penelitian terbaru aplikasi Android dapat digunakan untuk menerapkan Intrusion Prevention System pada jaringan perangkat Android berada. Telah dikembangkan HIDROID atau Host-based Intrusion Detection and Prevention System for Android dimana aplikasi ini dapat digunakan sebagai baik Intrusion Detection System (IDS) maupun Intrusion Prevention System (IPS) [11]. Cara kerja dengan menganalisis kondisi sumberdaya perangkat Android seperti CPU, memori, atau kondisi baterai. Sehingga konfigurasi IPS memang bisa dimungkinkan untuk dikembangkan pada perangkat smartphone Android. Selanjutnya aplikasi Android bisa berperan untuk IPS adalah dengan memanfaatkan VPNServices dan TCPDump untuk mengetahui lalu lintas data pada perangkat Android [12]. Dengan demikian aplikasi Android dapat menentukan apakah perilaku penggunaan Android termasuk berbahaya atau tidak dengan menggunakan notifikasi alarm. Dan bahkan aplikasi Android dengan kemampuan untuk mendeteksi dan mencegah serangan, untuk selanjutnya dapat dikembangkan untuk mendeteksi aplikasi malware [13]. Hal tersebut bisa tercapai dengan menggunakan metode Deep Learning sehingga Android dapat menentukan apakah aplikasi yang dicurigai adalah malware atau bukan.

Pada artikel penelitian ini akan dibahas mengenai pengembangan aplikasi remote berbasis Android untuk megendalikan konfigurasi IPS pada router MikroTik memanfaatkan teknologi IoT. Penelitian yang telah dilakukan ini memiliki kelebihan bahwa aplikasi Android yang dikembangkan fokus pada kemanan jaringan terutama pengelolaan Intrusion Prevention System pada router MikroTik serta pemanfaatan teknologi Internet of Things sebagai media kendali jarak jauh seperti penyimpanan Cloud Firebase dibantu dengan aplikasi agent berbasis web. Aplikasi yang dibangun memanfaatkan MikroTik API untuk bisa akses ke perangkat router MikroTik. Tujuan dari penelitian ini adalah mengembangkan aplikasi berbasis Android yang dapat mengendalikan router MikroTik dimana memiliki peran sebagai Intrusion Prevention System memanfaatkan teknologi Internet of Thing. Adapun batasan masalah pada penelitian yang dilakukan ini adalah pertama serangan pada jaringan yang diteliti meliputi Port Scanning, Brute Force tipe SSH dan FTP, serta Denial of Service tipe TCP SYN Flooding. Sedangkan perangkat router yang dikendalikan berbasis MikroTik dengan sistem operasi RouterOS versi 6 ke atas.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan

Keamanan sistem dan jaringan dilakukan untuk memonitor akses sistem dan jaringan serta mencegah penyalahgunaan sumber daya secara tidak sah. Tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Berdasarkan aktivitas, serangan pada jaringan terdiri dari dua jenis meliputi serangan pasif dan serangan aktif. Serangan pasif merupakan serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data, tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Sedangkan serangan aktif merupakan serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke dalam data stream atau dengan memodifikasi paket-paket yang melewati data stream.

2.2. Intrusion Prevention System

Intrusion Prevention System (IPS) adalah sistem yang mampu melakukan pencegahan terhadap paket data yang memiliki perilaku anomali atau mencurigakan. Kunci dari pencegahan adalah menerapkan aturan pada Firewall untuk menyaring paket data yang mencurigakan [1]. IPS juga memudahkan pengguna dalam mengetahui percobaan serangan jaringan karena adanya sistem log. Menurut VMWare, IPS merupakan perangkat keamanan jaringan yang setiap saat memantau lalu lintas jaringan dari aktivitas mencurigakan serta mengambil aksi untuk mencegah dengan cara menolak dan melaporkan kejadian.

Perbedaan antara IPS dan Intrusion Detection System (IDS) terletak pada aksi perangkatnya, apabila IDS secara sederhana mendeteksi paket data tanpa adanya aksi atau respon hanya memberitahu saja, sedangkan IPS lebih dari sekedar IDS dimana selain mendeteksi juga mencegah paket data yang mencurigakan dengan menolak serta melaporkan kejadian. Perangkat keras yang berperan sebagai IPS adalah perangkat firewall yang mampu melakukan filter terhadap banyaknya paket data yang berlalu lintas pada jaringan.

Terdapat tiga teknik dalam menerapkan IPS untuk mengidentifikasi suatu ancaman, meliputi:

- Signature-based merupakan penerapan IPS berdasarkan tanda signature pada ancaman yang sudah dikenal luas.
- Anomaly- based merupakan penerapan IPS yang memantau paket data dengan gerakan tidak normal. Teknik ini menetapkan gerakan tidak normal pada paket data dengan membandingkan sampel acak dengan standar yang ada.
- Policy-based merupakan teknik penerapan IPS yang tidak begitu populer dibandingkan Signature dan Anomali. Memanfaatkan aturan keamanan yang sebelumnya telah dijelaskan oleh perusahaan serta menolak koneksi yang sebelumnya melanggar aturan.

2.3. Basisdata Firebase

Firebase Realtime Database adalah salah satu cloud basis data yang diciptakan oleh Google. Data disimpan dalam bentuk JSON dan disesuaikan secara realtime ke setiap klien yang terhubung. Aplikasi ini menggunakan Firebase sebagai tempat penyimpanan data sekaligus untuk menghubungkan antara aplikasi desktop dengan aplikasi Android. Firebase menggunakan basis data *cloud* bernama NoAQL. Data disinkronisasi lintas client secara *real-time*, dan tetap terjaga meskipun aplikasi client telah offline. Firebase bisa diakses oleh aplikasi lintas platform seperti iOS, Android, Dan JavaScript SDK. Setiap client akan mendapatkan data share secara *realtime*, langsung, dan otomatis mendapatkan update data terbaru.

2.4. Aplikasi *Agent* Berbasis Web

Aplikasi agent berbasis web bertugas untuk mengambil data log MikroTik menggunakan API, untuk kemudian menyimpannya menuju basis data *realtime* Firebase. Berikut ini potongan kode bagaimana cara menyimpan data menuju Firebase berbasis web.

```
function writeUserData(userId, name, email,
imageUrl) {
  firebase.database().ref('users/'+
  userId).set({
    username: name,
    email: email,
    profile_picture : imageUrl
  });
}
```

3. METODE PENELITIAN

Terdapat lima tahapan utama pada penelitian yang dilakukan ini, meliputi Pengumpulan Data, Analisis, Perancangan, Implementasi, dan Pengujian seperti yang ditunjukkan pada Gambar 1.

3.1. Pengumpulan Data

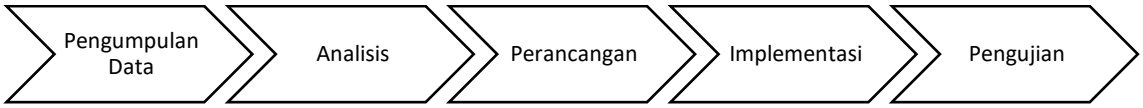
Pengumpulan data dilakukan dengan melakukan studi literatur. Data yang dimaksud adalah data konfigurasi IPS pada router MikroTik berdasarkan serangan Port Scanning, Brute Force tipe SSH dan FTP, serta Denial of Service tipe TCP Syn Flooding. Pengumpulan data studi literatur dilakukan dengan pengumpulan pustaka relevan, membaca, kemudian mencatat data konfigurasi. Sesuai dengan studi literatur yang telah dilakukan, terdapat konfigurasi tersendiri untuk mengatasi masing-masing jenis serangan. Dalam hal ini, untuk mengatasi serangan berupa Port Scanning maka digunakan fitur Port Scan Detect (PSD) pada konfigurasi Firewall Filter [14]. Kemudian untuk mengatasi serangan Brute Force, pada penelitian ini diuji coba serangan Brute Force baik pada SSH maupun FTP. Kedua jenis serangan Brute Force tersebut memiliki cara masing-masing untuk mengatasinya. Brute Force pada koneksi SSH dapat menggunakan rekayasa rule pada Firewall Filter secara bertahap untuk menolak koneksi SSH secara berkali-kali [15]. Sedangkan Brute Force tipe FTP dapat menggunakan fitur Destination Limit (Destination Limit) pada rule Firewall [16]. Untuk menahan serangan Denial of Service berupa SYN Flood bisa diatasi dengan menggunakan konfigurasi Firewall Raw dan ditambah fitur Destination Limit [17][18]. Cara bagaimana konfigurasi IPS pada router MikroTik menggunakan konfigurasi rule pada Firewall secara jelas telah dilakukan pada penelitian [19].

3.2. Analisis

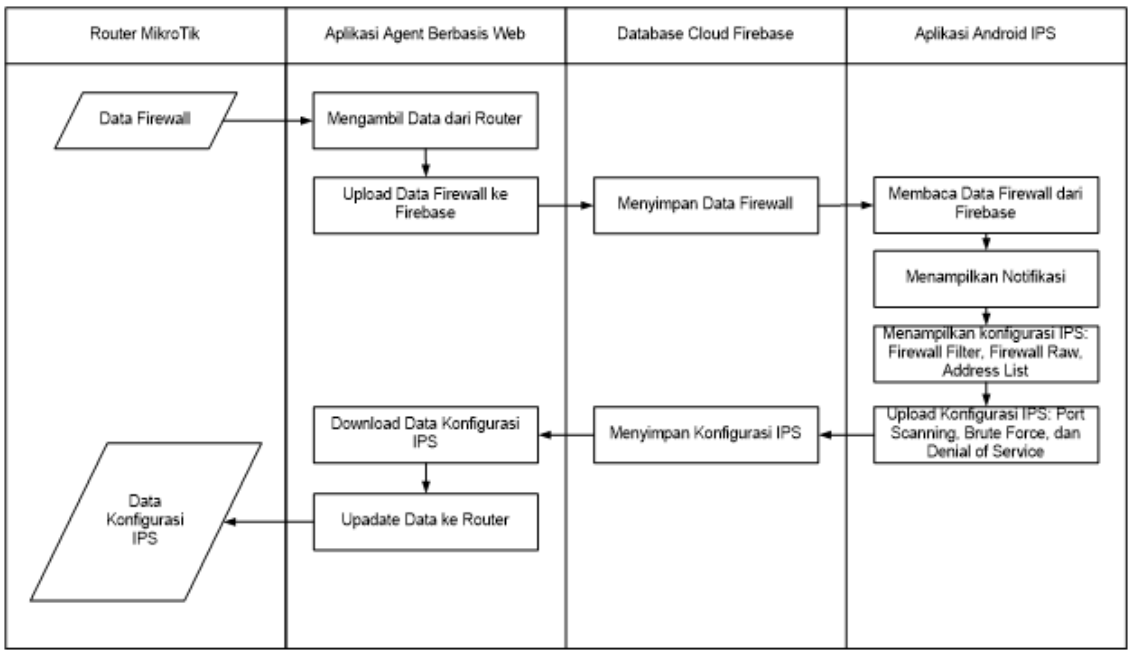
Agar aplikasi remote IPS berbasis Android ini bisa melakukan tugasnya dengan benar maka dimulai dengan mengaktifkan aplikasi agent dimana secara default, aplikasi agent mengambil data dari

router terlebih dahulu kemudian data disimpan menuju Firebase. Data yang telah berada pada Firebase dibaca oleh aplikasi Android, sehingga aplikasi Android dapat menampilkan konfigurasi IPS dari router berdasarkan data yang tersimpan pada Firebase. Apabila pengguna melakukan kendali terhadap data konfigurasi router melalui aplikasi Android, maka data-data konfigurasi tersebut ditulis di Firebase terlebih terlebih dahulu. Kemudian aplikasi agent akan membaca data konfigurasi dari Firebase untuk selanjutnya data konfigurasi tersebut diimplementasikan ke router MikroTik. Adapun proses bisnis aplikasi remote IPS berbasis Android secara umum ditampilkan pada Gambar 2.

.



Gambar 1. Tahapan Penelitian



Gambar 2. Proses Bisnis Aplikasi Remote IPS Android

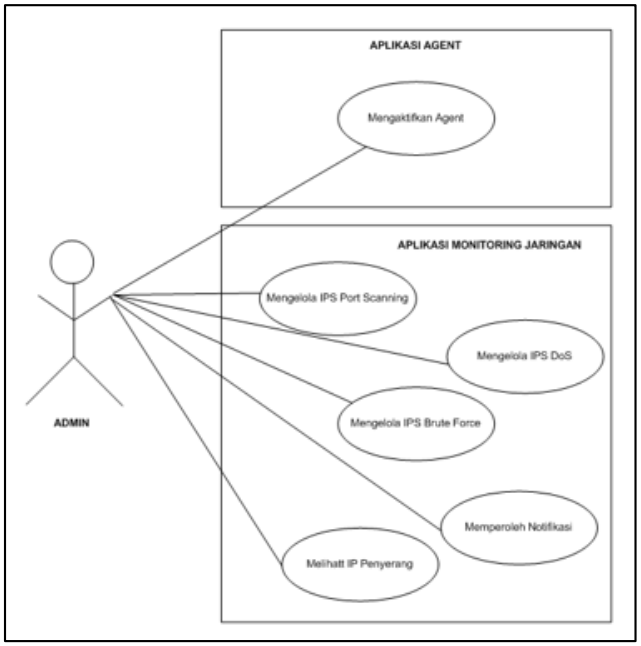
3.3. Perancangan

Perancangan pengembangan aplikasi dilakukan menggunakan pendekatan Unified Modeling Language meliputi Use Case Diagram, Class Diagram, Arsitektur Sistem, dan Struktur Data.

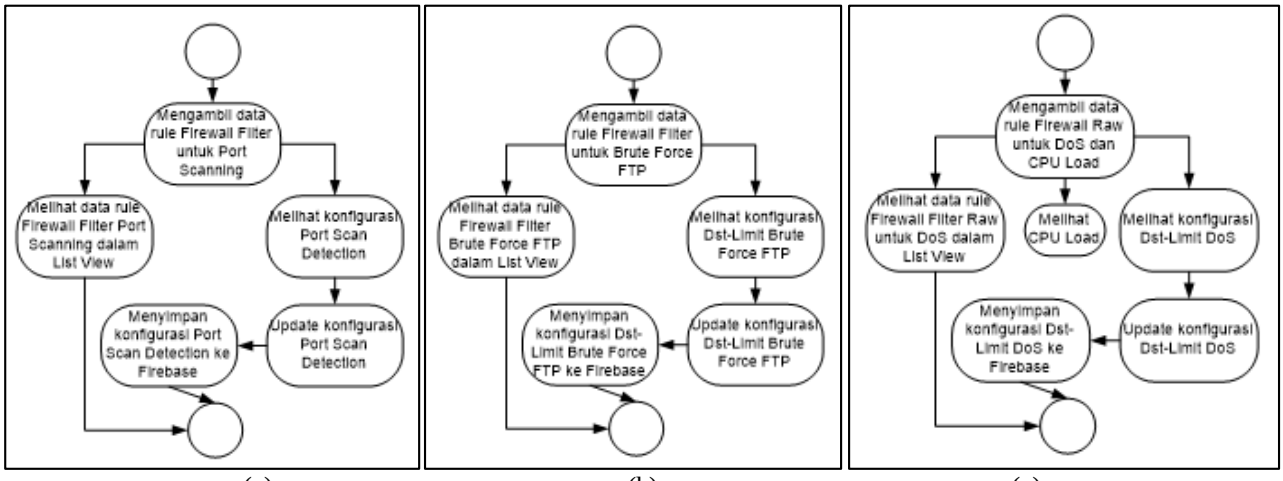
1. *Use Case Diagram*
   Use case terdiri dari enam case meliputi satu case pada boundary aplikasi agent berbasis web dan lima case pada boundary aplikasi remote konfigurasi IPS berbasis Android. Adapun case dominan meliputi mengelola IPS Port Scanning, mengelola IPS Brute Force, dan mengelola IPS DoS seperti yang ditampilkan pada Gambar 3.
2. *Activity Diagram*
   Sedangkan untuk diagram Activity, diagram yang dominan meliputi aktivitas mengelola IPS Port Scanning seperti pada Gambar 4(a), aktivitas mengelola IPS Brute Force tipe FTP pada Gambar 4(b), dan aktivitas mengelola IPS DoS seperti pada Gambar 4(c).
3. *Sequence Diagram*
   Berdasarkan diagram Activity yang diperoleh, maka diagram Sequence dominan pada aplikasi remote IPS ini diperlihatkan pada Gambar 5(a) untuk sequence mengelola IPS Port Scanning, Gambar 5(b) untuk sequence mengelola IPS Brute Force tipe FTP, dan Gambar 5(c) untuk sequence mengelola IPS DoS.
4. *Class Diagram*
   Dikarenakan dibutuhkan aplikasi agent berbasis web dalam mengembangkan aplikasi remote konfigurasi IPS berbasis Android maka class yang digunakan berada pada dua platform yang berbeda. Sedangkan diagram class untuk aplikasi remote berbasis Android untuk control konfigurasi IPS ditampilkan pada Gambar 6. Class untuk view terdiri dari 5 class meliputi activity_portscanning.xml, activity_bruteforcessh.xml, activity_bruteforceftp.-xml, activity_dosattack.xml, dan activity_addresslist.xml. Sedangkan untuk controller terdapat 5 class meliputi portscanning.kt, bruteforcessh.kt,

bruteforceftp.kt, dosattack.kt, dan addresslistactivity.kt. Dan class untuk model terdiri 6 class meliputi rulescanning.kt, rulebruteforcessh.kt, rulebruteforceftp.kt, ruledosattack.kt, resource.kt, dan addresslist.kt. Sebagai entitas terakhir untuk menyimpan data digunakan Firebase Realtime Database.

5. Arsitektur Sistem
   Gambar 7 merupakan arsitektur sistem bagaimana aplikasi remote berbasis Android berjalan. Agar aplikasi remote Android bisa berjalan harus diaktifkan aplikasi agentnya terlebih dahulu. Pengguna hanya satu yaitu Admin dimana memiliki akses pada dua aplikasi yaitu aplikasi agen berbasis web dan aplikasi remote konfigurasi IPS berbasis Android. Aplikasi agent bertanggung jawab untuk mengambil data dari perangkat router MikroTik untuk disimpan ke Firebase serta sebaliknya mengambil data dari Firebase untuk diterapkan menuju router MikroTik. Aplikasi remote konfigurasi IPS bisa melihat data konfigurasi IPS yang tersimpan di Firebase dan juga dapat mengubah konfigurasi IPS dengan update data konfigurasi yang tersimpan di Firebase.

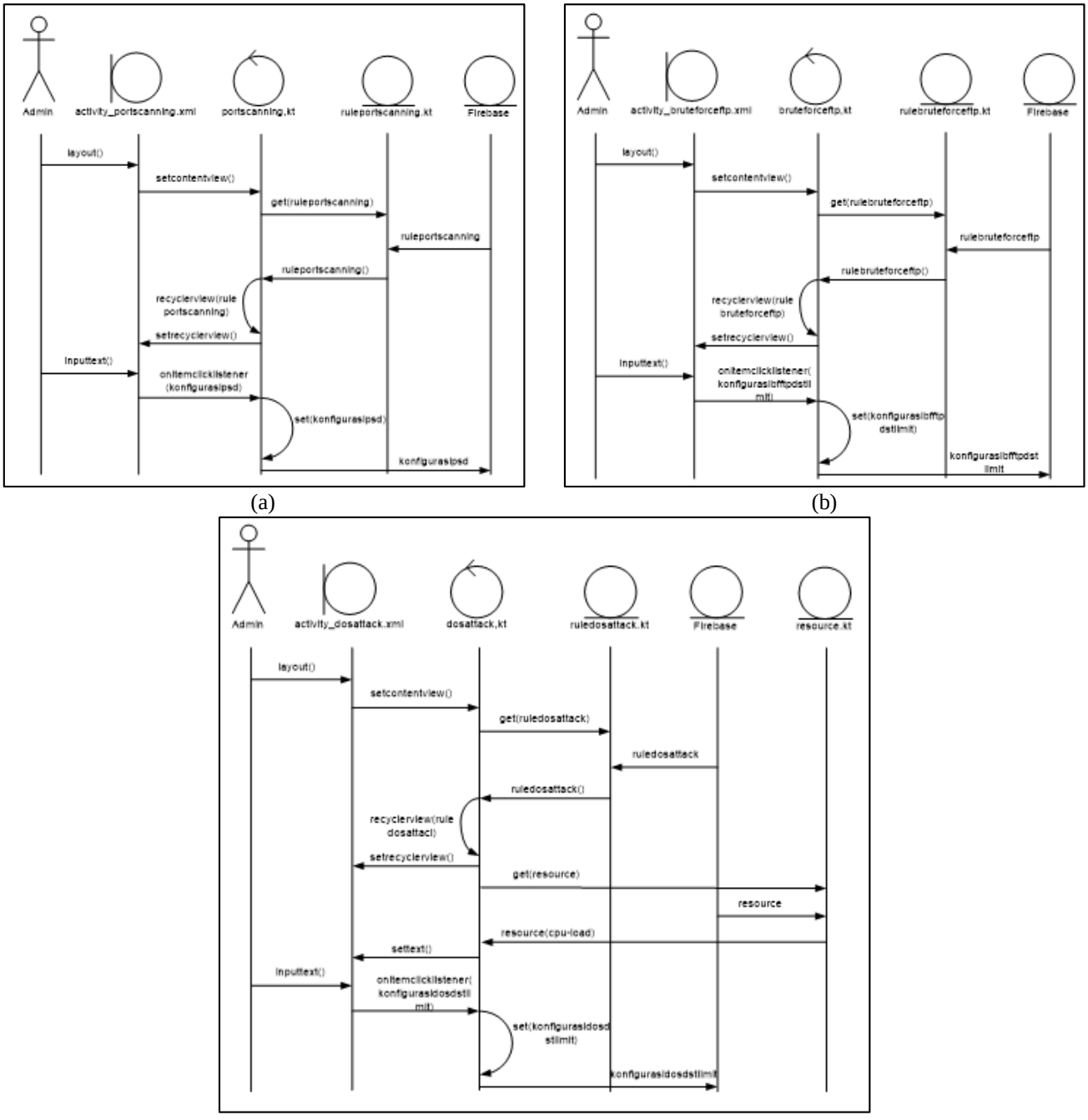


Gambar 3. Diagram Use Case Aplikasi Remote Konfigurasi IPS Berbasis Android

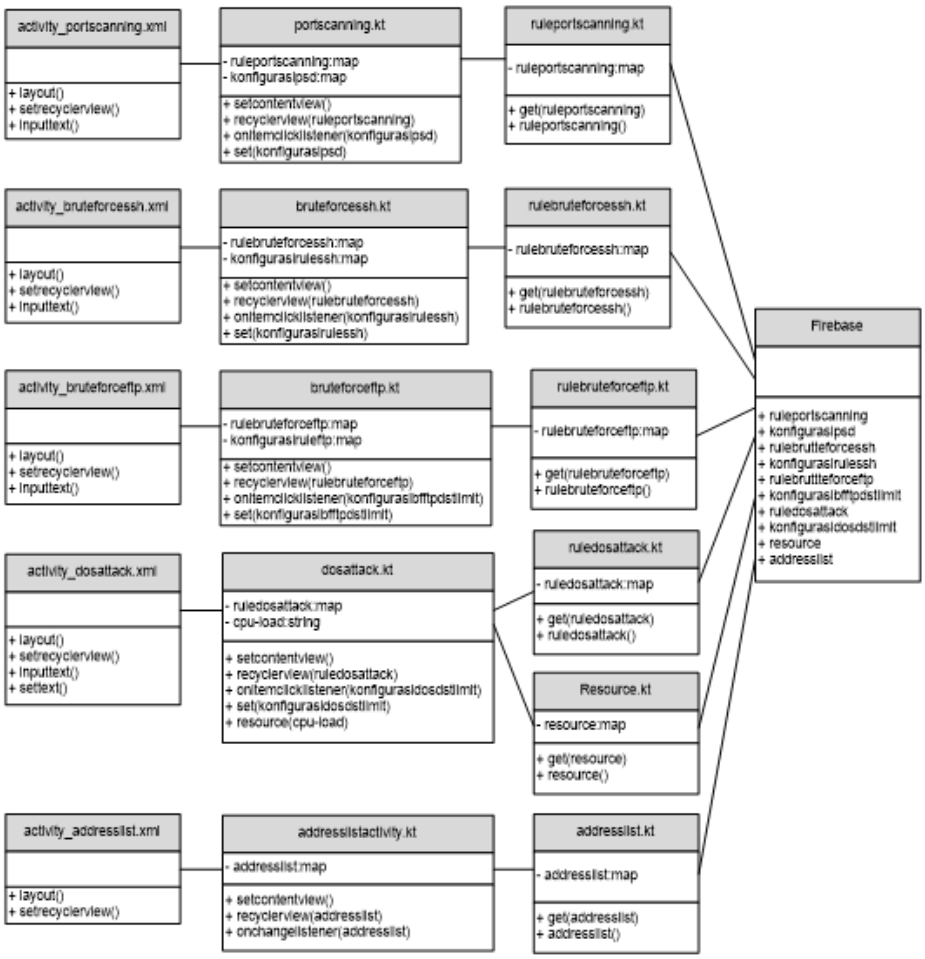


(a) (b) (c)

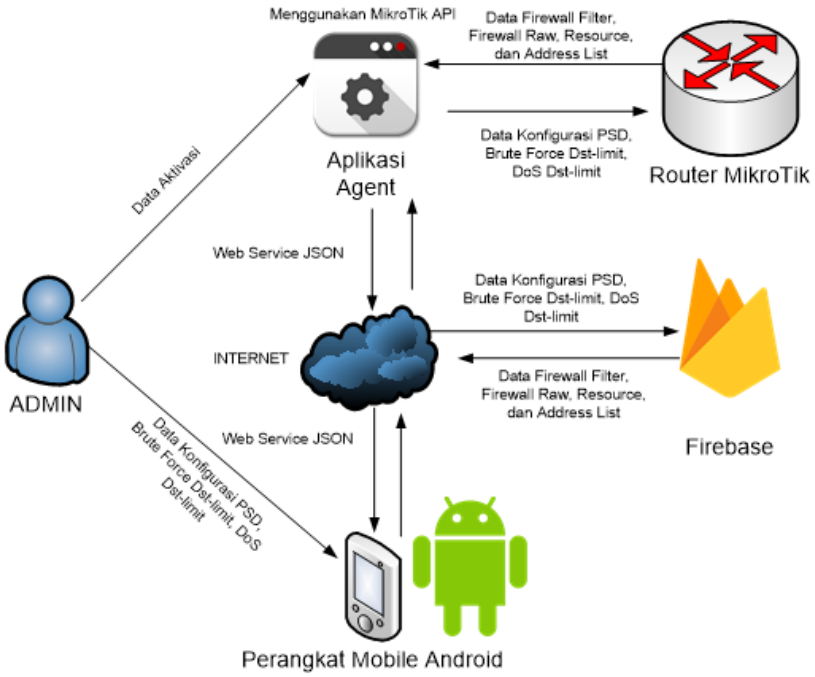
Gambar 4. Diagram Activity Aplikasi Remote Konfigurasi IPS Berbasis Android
(a) IPS Port Scanning (b) IPS Brute Force Tipe FTP (c) IPS DoS



Gambar 5. Diagram Sequence Aplikasi Remote Konfigurasi IPS Berbasis Android
(a) IPS Port Scanning (b) IPS Brute Force Tipe FTP (c) IPS DoS



Gambar 6. Diagram Class Aplikasi Remote Konfigurasi IPS Berbasis Android



Gambar 7. Arsitektur Sistem Pada Aplikasi Remote Konfigurasi IPS Berbasis Android

6. Struktur Data

Pada penelitian ini dimanfaatkan basis data non relasi dimana antar tabel penyimpanan tidak ada relasi sama sekali. Sesuai dengan class Firebase pada diagram class Gambar 6 terdapat 10 metode untuk membuat objek data meliputi ruleportscanning(), konfigurasipsd(), rulebruteforcessh(), konfigurasirulessh(), rulebruteforceftp(), konfigurasibfftpdstlimit(), ruledosattack(), konfigurasidosdstlimit(), resource(), dan addresslist(). Untuk mendukung teknologi Internet of Things digunakan penyimpanan online berupa *cloud* Firebase. Sebagai penyimpan informasi konfigurasi IPS berupa data rule Firewall Filter dan rule Firewall Raw, data CPU Load dari Resource, serta data alamat IP yang mencurigakan dari Address List maka digunakan Firebase fitur Firestore sebagai media penyimpanannya. Adapun struktur data pada Firebase Firestore ditunjukkan pada Tabel 1.

Tabel 1. Struktur Data Firestore untuk Monitoring Data Konfigurasi IPS

Collection	Document (tipe data)	Fungsi	Method
networkipscontroller	Addresslist (String)	Menyimpan kumpulan data address-list dimana menyimpan alamat IP penyerang	addresslist()
	Portscan (String)	Menyimpan kumpulan rule firewall filter untuk IPS port scanning	konfigurasipsd()
	Bruteforcessh (String)	Menyimpan kumpulan rule firewall filter untuk IPS brute force tipe SSH	konfigurasirulessh()
	Bruteforcefp (String)	Menyimpan kumpulan rule firewall filter untuk IPS brute force tipe FTP	konfigurasibfftpdstlimit()
	Dosattack (String)	Menyimpan kumpulan rule firewall raw untuk IPS denial of service	konfigurasidosdstlimit()
	Resource (String)	Menyimpan kumpulan informasi resource termasuk di dalamnya CPU load	resource()

Sedangkan untuk melakukan pengendalian remote pada konfigurasi IPS meliputi konfigurasi Port Scan Detection, Destination Limit baik untuk serangan Brute Force tipe FTP maupun Destination Limit untuk serangan Denial of Service, dan Jumlah Filter SSH menggunakan penyimpanan Firebase fitur Real-time Database. Tabel 2 merupakan struktur data dari Firebase Real-time Database yang digunakan.

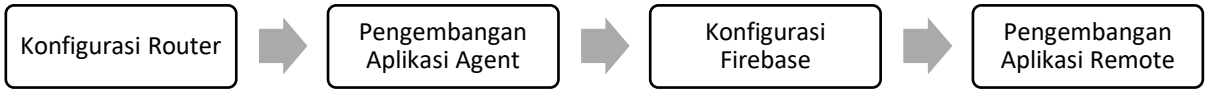
Tabel 2. Struktur Data Real-Time Database untuk Remote Data Konfigurasi IPS

Collection	Document (tipe data)	Fungsi	Method
portscandetection	threshold (number)	Menyimpan nilai threshold PSD	ruleportscanning()
	interval (number)	Menyimpan nilai interval pada PSD	
	lpw (number)	Menyimpan nilai low port weight PSD	
	hpw (number)	Menyimpan nilai high port weight PSD	
bruteforceftpdst-limit	rate (number)	Menyimpan nilai rate pada dst-limit	rulebruteforceftp()
	burst (number)	Menyimpan nilai burst pada dst-limit	
	exp (number)	Menyimpan nilai expired time pada dst-limit	
dosattackdst-limit	rate (number)	Menyimpan nilai rate pada dst-limit	ruledosattack()
	burst (number)	Menyimpan nilai burst pada dst-limit	
	exp (number)	Menyimpan nilai expired time pada dst-limit	
bruteforcessh	jumlahssh (number)	Menyimpan nilai jumlah filter SSH	rulebruteforcessh()

4. HASIL DAN PEMBAHASAN

4.1. Implementasi

Implementasi dilakukan dengan empat sub-tahapan meliputi Konfigurasi Router MikroTik, Pembuatan Aplikasi Agent Berbasis Web, Konfigurasi Firebase, dan kemudian Pengembangan Aplikasi Remote IPS Berbasis Android seperti pada Gambar 8.



Gambar 8. Sub-tahapan pada Tahap Implementasi

Berikut detail implementasi pada setiap tahapannya.

1. Konfigurasi Router

   Pada penelitian ini, router MikroTik harus dikonfigurasi terlebih dahulu aturan awal dari Firewall untuk penerapan IPS. Sebelum melakukan konfigurasi awal, disiapkan akun Admin untuk verifikasi masuk router. Kemudian dilakukan konfigurasi Firewall meliputi rule

Firewall Filter untuk menangani serangan Port Scanning, Brute Force tipe SSH maupun tipe FTP, dan Firewall Raw untuk menangani serangan Denial of Service tipe SYN Flood [16].

2. Pengembangan Aplikasi Agent
   Aplikasi agent dikembangkan pada lingkungan web menggunakan framework Laravel 7. Dimanfaatkan library RouterOS API versi PHP yang dikembangkan oleh BenMenking/routeros-api agar aplikasi agent bisa mengakses data router MikroTik. Agar aplikasi agent bisa mengakses Firebase maka digunakan library Firebase-Laravel dari kreait/laravel-firebase. Selanjutnya agar aplikasi agent bisa aktif secara terus menerus, maka dimanfaatkan JavaScript fungsi SetInterval() dengan delay 15000ms.
3. Konfigurasi Firebase
   Dengan proyek Firebase yang sama, digunakan dua fitur Firebase untuk menyimpan data konfigurasi IPS meliputi Firestore dan Real-time Database. Firestore digunakan untuk memonitor data konfigurasi Firewall, sedangkan Real-time Database digunakan untuk mengendalikan detail konfigurasi Firewall.
4. Pengembangan Aplikasi Remote
   Aplikasi remote berbasis Android menggunakan bahasa pemrograman Kotlin pada lingkungan Android Studio.

Pengujian dilakukan dalam dua tahap meliputi pengujian fungsional aplikasi dan pengujian kinerja IPS. Pengujian fungsional melakukan pengujian aplikasi Android berdasarkan fungsi-fungsi yang telah direncanakan sebelumnya. Sedangkan pengujian kinerja IPS melakukan pengujian terhadap kinerja aplikasi dalam mengendalikan router MikroTik sebagai perangkat IPS. Pengujian melibatkan responden dari Puskom PSDKU Polinema di Kota Kediri.

1. Pengujian Fungsional Aplikasi
   Tabel 3 merupakan detail variabel uji coba untuk pengujian kebutuhan fungsional dari aplikasi monitoring jaringan berbasis Android.

Tabel 3. Skenario Pengujian Fungsional Aplikasi Remote Android untuk Konfigurasi IPS

No.	Skenario	Hasil
1	Mengaktifkan aplikasi Agent	Data berhasil diakses dari router dan disimpan ke Firebase
2	Mengelola IPS Port Scanning	- Berhasil melihat rule Firewall untuk Port Scanning - Berhasil update konfigurasi Firewall untuk Port Scanning
3	Mengelola IPS Brute Force SSH	- Berhasil melihat rule Firewall untuk Brute Force tipe SSH - Berhasil update konfigurasi Firewall untuk Brute Force tipe SSH
4	Mengelola IPS Brute Force FTP	- Berhasil melihat rule Firewall untuk Brute Force tipe FTP - Berhasil update konfigurasi Firewall untuk Brute Force tipe FTP
5	Mengelola IPS Denial of Service	- Berhasil melihat rule Firewall untuk Denial of Service tipe SYN Flood - Berhasil melihat persentase CPU Load router - Berhasil update konfigurasi Firewall untuk Denial of Service tipe SYN Flood
6	Melihat IP penyerang	Berhasil melihat daftar alamat IP penyerang
7	Memperoleh notifikasi	Berhasil menerima notifikasi ketika ada penyerang baru

Pengujian fungsional dilakukan oleh lebih dari satu responden, maka akan diambil persentase rata-rata keberhasilan untuk setiap variabel pengujian seperti pada rumus 1.

$$APK = \frac{NK}{NR} \times 100 \quad \text{...(1)}$$

Keterangan:
APK = persentase rata-rata fungsi yang berhasil
NK = jumlah penguji yang menjawab berhasil
NR = jumlah penguji

2. Pengujian Kinerja IPS
   Pengujian kinerja bertujuan untuk mengukur kemampuan aplikasi Android untuk bisa mengendalikan konfigurasi router MikroTik sebagai IPS, sehingga router mampu menahan serangan berupa Port Scanning, Brute Force, dan Denial of Service. Pengujian serangan dilakukan dengan bantuan aplikasi seperti pada Tabel 4.

Tabel 4. Skenario Pengujian Kinerja Aplikasi

Collection	Document	Fungsi
Port Scanning	Nmap	- 10 kali percobaan - Menggunakan 10 port
Brute Force tipe SSH	Hydra	- 10 kali percobaan - Menggunakan 10 variabel
Brute Force tipe FTP	Hydra	- 10 kali percobaan - Menggunakan 10 variabel
Denial of Service tipe SYN Flood	Hping3	- 10 kali percobaan - Selama 3 menit - Menggunakan 1000 paket

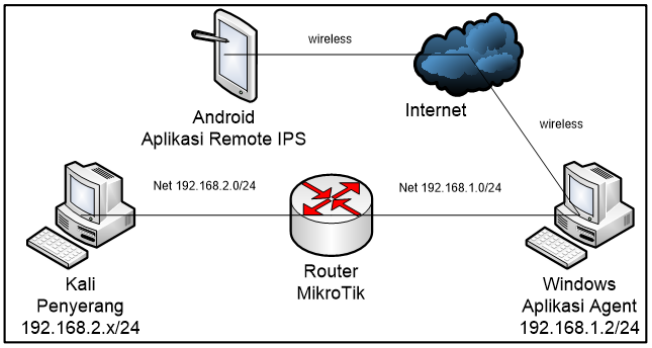
Pengukuran kinerja dihitung dari keberhasilan router MikroTik dalam menolak percobaan serangan dimana hasil perhitungan akan dipresentasikan berdasarkan nilai persentase sesuai rumus 2.

$$APT = \frac{NT}{NS} \times 100 \quad ...(2)$$

Keterangan:
APT = persentase rata-rata berhasil menolak serangan
NT = jumlah percobaan berhasil ditolak
NS = jumlah percobaan

4.2. Hasil Implementasi

Untuk melakukan implementasi aplikasi maka dibangun *testbed* agar aplikasi yang dibangun dan skenario pengujian dapat berjalan. *Testbed* dibangun dengan kondisi yang relevan dimana dapat digunakan untuk dua jenis pengujian sekaligus, meliputi pengujian fungsional aplikasi remote dan pengujian kinerja IPS. Agar pengujian fungsional bisa berjalan maka diperlukan aplikasi remote berbasis Android dimana aplikasi agent berbasis web telah aktif dan terkoneksi ke internet serta sekaligus aplikasi agent tersebut telah terhubung ke router MikroTik pada jaringan lokal. Selanjutnya agar pengujian kinerja IPS hasil kendali remote bisa berjalan maka disiapkan sebuah komputer personal yang berperan sebagai penyerang. Adapun topologi *testbed* untuk skenario pengujian ditampilkan pada Gambar 9.



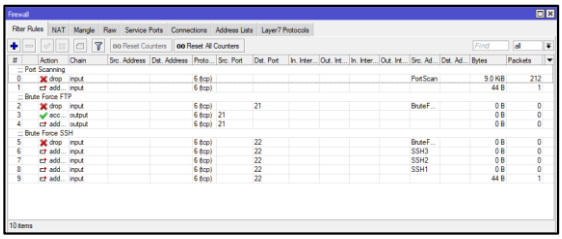
Gambar 9. Topologi Testbed untuk Implementasi dan Pengujian

Berikut ini penjelasan detail mengenai peran setiap device pada *testbed*:

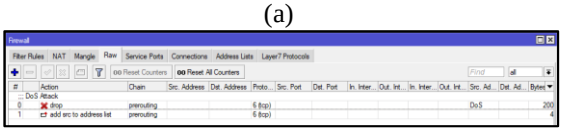
a. Aplikasi remote pengendali konfigurasi IPS berbasis Android terhubung internet untuk membaca konfigurasi IPS serta menulis update konfigurasi IPS yang tersimpan pada Firebase baik pada Firestore maupun Real-time Database.
b. Internet digunakan untuk komunikasi data antara aplikasi remote Android dengan aplikasi agent berbasis web melalui *cloud* Firebase, sehingga konsep Internet of Things dapat diterapkan.
c. Aplikasi agent berbasis web terinstal pada komputer bersistem operasi Windows 10. Aplikasi agent berperan sebagai perantara untuk membaca dan mengupdate konfigurasi IPS pada router MikroTik menuju media penyimpan data *cloud* Firebase.
d. Router MikroTik menjadi objek eksekusi konfigurasi IPS (aktuator IPS) dalam mencegah serangan meliputi Port Scanning, Brute Force, dan Denial of Service. Router MikroTik dapat diakses melalui koneksi API yang diterapkan oleh aplikasi Agent berbasis web.
e. Penyerang adalah komputer bersistem operasi Kali dimana memiliki peran untuk menguji IPS pada router MikroTik meliputi serangan Port Scanning, Brute Force dan Denial of Service.

Setelah *testbed* dibangun, kemudian diberikan konfigurasi awal IPS pada router MikroTik dengan sekumpulan aturan pada Firewall Filter maupun Firewall Raw seperti pada Gambar 8. Berikut ini penjelasan detail mengenai konfigurasi awal pada router.

a. Gambar 10(a) merupakan konfigurasi IPS serangan Port Scanning yang terdiri dua baris aturan Firewall Filter meliputi aturan Drop dan aturan Add Src To Address List. Serangan Brute Force SSH yang terdiri lima baris aturan Firewall Filter meliputi aturan Drop dan empat aturan Add Src To Address List. Dan serangan Brute Force FTP yang terdiri tiga baris aturan Firewall Filter meliputi aturan Drop, aturan Accept, dan aturan Add Dst To Address List.
b. Gambar 10(b) serangan Denial of Service yang terdiri dua baris aturan Firewall Raw meliputi aturan Drop dan aturan Add Src To Address List.



(a)

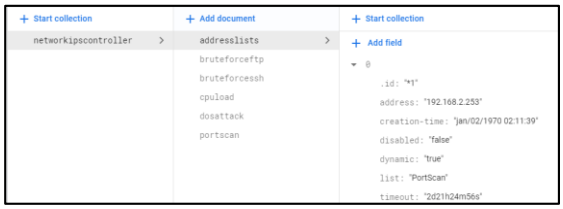


(b)

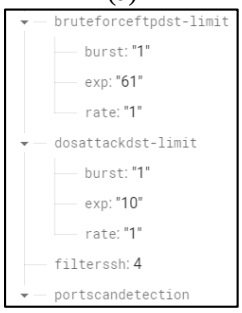
Gambar 10. Konfigurasi Awal IPS pada Firewall Router (a) Filter Rule (b) Raw

Adapun implementasi struktur data pada Firebase menggunakan Firestore sebagai monitor aturan Firewall dan Real-time Database sebagai remote konfigurasi aturan Firewall ditunjukkan pada Gambar 11.

a. Gambar 11(a) merupakan tampilan penyimpanan Firebase Firestore meliputi satu collection dan enam document.
b. Gambar 11(b) merupakan tampilan penyimpanan Firebase Real-time meliputi empat field.



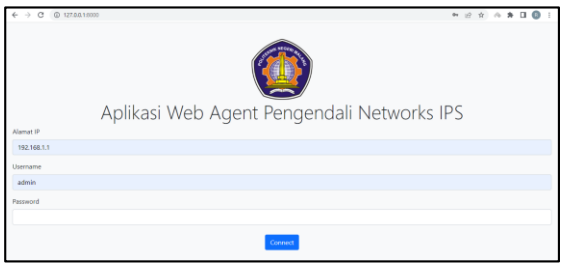
(a)



(b)

Gambar 11. Implementasi Struktur Data Firebase (a) Firestore (b) Real-time

Implementasi pengembangan aplikasi agent berbasis web yang dikembangkan pada framework Laravel 7 dengan menerapkan library RouterOS API PHP dan library Laravel-Firebase. Proses *looping* eksekusi menggunakan fungsi SetInterval() dengan delay 15000ms sehingga data akan di-update untuk setiap 15 detik. Pada tampilan Gambar 12 terdapat tiga form yang terdiri dari form alamat ip dari router, username akun router, dan password akun router. Untuk aktivasi tinggal klik tombol Connect. Gambar 13 merupakan tampilan Aplikasi Remote Android.



Gambar 12. Tampilan Aplikasi Agent Berbasis Web

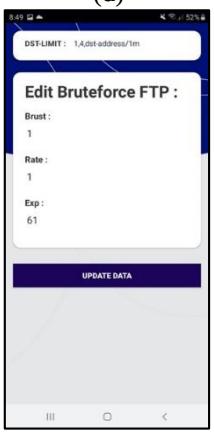
(a)

(b)

(c)

(d)

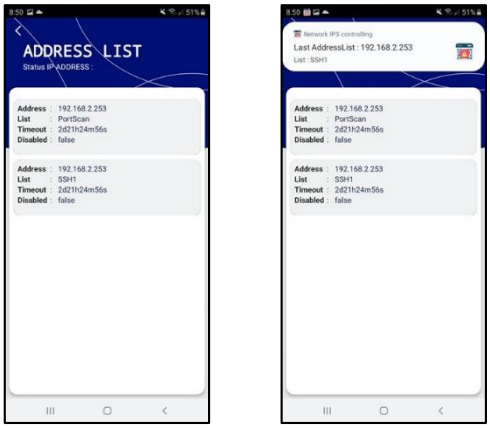
(e)



(f)

(g)

(h)



(i) (j)

Gambar 13. Tampilan Aplikasi Remote Berbasis Android
(a) Tampilan Menu (b) Konfigurasi IPS Port Scanning (c) Update PSD IPS Port Scanning (d) Konfigurasi IPS Brute Force SSH (e) Konfigurasi IPS Brute Force FTP (f) Update Destination Limit Brute Force FTP (g) Konfigurasi IPS Denial of Service (h) Update Destination Limit Denial of Service (i) Tampilan IP Penyerang (j) Tampilan Notifikasi Serangan

4.3. Pembahasan Pengujian Fungsional Aplikasi

Pengujian fungsional aplikasi melibatkan 2 orang responden sebagai penguji aplikasi dari Puskom PSDKU Polinema di Kota Kediri. Pengujian dilakukan dengan memberikan kendali konfigurasi IPS dari aplikasi Android sesuai kebutuhan fungsional yang direncanakan. Pengujian fungsional dilakukan secara 4 tahapan meliputi persiapan testbed seperti pada Gambar 9, skenario pengujian seperti pada Tabel 3, pengisian kuisioner oleh responden, dan penarikan kesimpulan seperti pada Gambar 14. Tabel 5 merupakan hasil pengujian fungsional aplikasi remote Android untuk konfigurasi IPS dimana hasilnya fungsi-fungsi aplikasi secara umum berhasil berjalan mencapai 91.67%. Penilaian pengujian menggunakan rumus (1). Terdapat ketidakberhasilan minor pada jalannya fungsi aplikasi yaitu untuk melakukan update jumlah rule filter pada SSH.

Gambar 14. Langkah Pengujian Fungsional

Tabel 5. Hasil Pengujian Fungsional Aplikasi

Skenario	Hasil yang diharapkan	Rata-rata (%)	Kesimpulan
Mengaktifkan aplikasi Agent	Data berhasil aktif dan tampil	100	Berhasil
Mengelola IPS Port Scanning	Berhasil melihat rule Firewall Filter IPS Port Scanning	100	Berhasil
	Berhasil update konfigurasi PSD	100	Berhasil
Mengelola IPS Brute Force SSH	Berhasil melihat rule Firewall Filter IPS Brute Force SSH	100	Berhasil
	Berhasil update konfigurasi jumlah Filter SSH	0	Tidak Berhasil
Mengelola IPS Brute Force FTP	Berhasil melihat rule Firewall Filter IPS Brute Force FTP	100	Berhasil
	Berhasil update konfigurasi Brute Force Dst-limit	100	Berhasil
Mengelola IPS Denial of Service	Berhasil melihat rule Firewall Filter IPS Denial of Service	100	Berhasil
	Berhasil melihat persentase CPU Load	100	Berhasil
	Berhasil update konfigurasi DoS Dst-limit	100	Berhasil
Melihat IP penyerang	Berhasil melihat IP penyerang melalui daftar Address List	100	Berhasil
Memperoleh notifikasi	Berhasil notifikasi aktif ketika ada penyerang baru	100	Berhasil
Rata-rata keseluruhan (%)		**91.67**	**Berhasil**

Terdapat fungsi yang tidak berhasil adalah fungsi untuk melakukan update konfigurasi jumlah filter SSH. Nilai jumlah filter SSH bisa diubah pada data Firebase Real-time Database. Namun penggunaan logika yang telah dibangun pada aplikasi Agent dalam membuat jumlah rule filter SSH pada Firewall router MikroTik tidak berhasil berjalan dengan baik.

4.4. Pembahasan Pengujian Kinerja IPS

Pengujian kinerja IPS bertujuan untuk menguji kinerja router MikroTik dalam menjalankan konfigurasi IPS hasil kendali dari aplikasi Android secara remote. Berdasarkan testbed Gambar 9, pengujian dilakukan dengan memberikan serangan dari PC Kali sebagai penyerang menuju ke router MikroTik sesuai skenario pada Tabel 4. Pengujian kinerja dilakukan secara 3 tahapan meliputi persiapan testbed seperti pada Gambar 9, skenario pengujian seperti pada Tabel 4, dan penarikan hasil seperti pada Gambar 15. Pengujian Kinerja IPS ditampilkan dengan persentase sesuai rumus (2). Tabel 6 merupakan hasil pengujian kinerja IPS dimana menggunakan skenario serangan sesuai

rencana pengujian. Secara keseluruhan keberhasilan IPS pada router MikroTik hasil konfigurasi pada aplikasi remote mencapai 95%.

Gambar 15. Langkah Pengujian Kinerja IPS

Tabel 6. Hasil Pengujian Kinerja IPS

Skenario	Jumlah uji coba	Gagal	Berhasil	Persentase
Port Scanning	10	0	10	100
Brute Force SSH	10	1	9	90
Brute Force FTP	10	10	0	0
DoS	10	0	10	100
Rata-rata keseluruhan (%)				**72.5**

Kegagalan satu kali dalam menolak serangan FTP dikarenakan router perlu memahami rule konfigurasi terlebih dahulu, sehingga satu kali serangan yang dilakukan saat pertama kali akan lolos dari IPS router. Hal tersebut efek dari konfigurasi IPS pada Brute Force dimana bergantung pada jumlah paket yang diterima router baik paket melalui FTP sehingga router memerlukan waktu adaptasi. Sedangkan karena fungsi kendali konfigurasi Brute Force SSH tidak berhasil pada pengujian fungsional sebelumnya, sehingga kinerja gagal dalam membendung serangan Brute Force SSH.

5. KESIMPULAN DAN SARAN

Telah berhasil dikembangkan aplikasi berbasis Android yang dapat mengendalikan router MikroTik dimana memiliki peran sebagai Intrusion Prevention System memanfaatkan teknologi Internet of Things dengan fungsi-fungsi sebagai berikut Admin mengaktifkan aplikasi Web Agent, mengelola konfigurasi IPS Port Scanning, mengelola konfigurasi IPS Brute Force tipe FTP sedangkan konfigurasi IPS Brute Force tipe SSH hanya bisa dilihat saja, mengelola konfigurasi IPS Denial of Service, melihat alamat IP penyerang, serta memperoleh notifikasi serangan. Hasil pengujian fungsional aplikasi remote Android untuk konfigurasi IPS memiliki keberhasilan fungsional secara keseluruhan mencapai lebih dari 91.67%, sedangkan hasil pengujian kinerja IPS pada router MikroTik setelah dikendalikan oleh aplikasi remote Android secara keseluruhan mencapai 72.5%.

Sebagai pengembangan untuk penelitian selanjutnya perlu dilakukan analisis untuk mengukur kinerja respon Router MikroTik terhadap nilai data yang diinputkan dari aplikasi IPS Android menuju Firebase Realtime Database.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Politeknik Negeri Malang dan Bagian LPPM di PSDKU Politeknik Negeri Malang di Kediri yang telah memberikan bantuan dalam pelaksanaan kegiatan penelitian ini melalui DIPA 2022. Tak lupa kami sampaikan terima kasih pula kepada tim mahasiswa yang membantu dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] F. Wahyudi and L. T. Utomo, "Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang," *Edumatic J. Pendidik. Inform.*, vol. 5, no. 1, pp. 60–69, 2021.

[2] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *It J. Res. Dev.*, vol. 3, no. 1, pp. 104–114, 2018.

[3] G. T. Irawan, M. Djaohar, and M. Ficky Duskarnaen, "Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 2, no. 1, pp. 27–32, 2018.

[4] B. Jaya, Y. Yunus, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 5–9, 2020.

[5] M. Fakhmi and L. M. Gultom, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)," *Semin. Nas. Ind. dan Teknol.*, pp. 260–277, 2021.

[6] H. Haeruddin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS," *J. Media Inform. Budidarma*, vol. 5, no. 3, p. 848, 2021.

[7] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *J. Big Data*, vol. 6, no. 1, 2019.

[8] M. Risaldi and A. Ayuningtyas, "Simulasi Pengendalian Router Mikrotik Menggunakan Android," *Compiler*, vol. 7, no. 1, pp. 46–53, 2018.

[9] Y. H. Tasanah Assakur, M. S. Fahrudin, and F. Ferdiansyah, "Implementasi API Mikrotik untuk Management Router Berbasis Android (Studi Kasus: PT Sigma Adi Perkasa)," *J. Sains dan Inform.*, vol. 6, no. 1, pp. 92–101, 2020.

[10] A. Imae *et al.*, "Router Control Function Using IoT Device Supported OpenFlow Switch in IP over AWG-STAR Network," *25th Opto-Electronics Commun. Conf. OECC 2020*, pp. 16–18, 2020.

[11] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed, "HIDROID: Prototyping a Behavioral Host-Based Intrusion Detection and Prevention System for Android," *IEEE Access*, vol. 8, pp. 23154–23168, 2020.

[12] Y. Chen, "Research on Application System of Remote-Control Computer of Android Mobile Phone," *J. Phys. Conf. Ser.*, vol. 1992, no. 2, 2021.

[13] R. Ali, A. Ali, F. Iqbal, M. Hussain, and F. Ullah, "Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review," *Secur. Commun. Networks*, vol. 2022, 2022.

[14] A. D. Susilo, "Ids Implementation With Mikrotik," 2017.

[15] O. Fajar and A. Zaky, "Prevention Login Brut eforce MikroTIK," 2016.

[16] T. Y. May, "How to Protecting your Mikrotik Router From Brutes-Force Attack • Where I Come From ?," 2017.

[17] A. Giordano, "No Title," in *Reducing the impact of DoS attacks with MikroTik RouterOS*, 2015.

[18] M. J. Purba and A. G. P. Simanjuntak, "Pengamanan Mikrotik Routerboard Dari Serangan Keamanan Dengan Notifikasi Bot Telegram," *Maj. Ilm. METHODA*, vol. 11, no. 3, pp. 241–246, 2021.

[19] Rinanza Zulmy Alhamri, Kunti Eliyen, and Agustono Heriadi, "Pemanfaatan Api Client Berbasis Python Untuk Konfigurasi Ips Pada Router Mikrotik," *J. Tek. Ilmu Dan Apl.*, vol. 3, no. 2, pp. 162–172, 2022.