JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 3, November 2025, hal. 788~793
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Model Implementasi *Firewall* MikroTik dalam Pengelolaan Trafik dan Keamanan Jaringan

[1]Abraham Cornelius Dachi, [2]Handrie Noprisson
[1] Fakultas Teknik dan Informatika, Universitas Dian Nusantara, Indonesia
[1]411211089@mahasiswa.undira.ac.id; [2]handrie.noprisson@dosen.undira.ac.id

Article Info

Article history:

Received, 2025-11-21
Revised, 2025-12-01
Accepted, 2025-12-09

Kata Kunci:

Firewall Mikrotik,
Keamanan Jaringan,
Manajemen Trafik,
Cybersecurity,
Network Performance

ABSTRAK

Penelitian ini bertujuan untuk menganalisis peran implementasi *firewall* pada MikroTik RouterOS dalam meningkatkan keamanan jaringan dan pengelolaan trafik di lingkungan CV. Prima Dinamika Mandiri. Infrastruktur jaringan perusahaan terdiri atas router penyedia layanan internet (*router* ISP), router MikroTik sebagai *firewall* dan *gateway* utama, *switch* jaringan untuk distribusi LAN internal, beberapa access point di area kerja, perangkat klien berupa laptop, PC, dan server, serta printer sharing pada tiap ruangan. Implementasi firewall dilakukan melalui konfigurasi *filtering rules*, proteksi *brute force*, Layer 7 *filtering*, *Network Address Translation* (NAT), serta *Quality of Service* (QoS) untuk meminimalkan ancaman keamanan dan mengoptimalkan distribusi trafik jaringan. Hasil pengujian menunjukkan adanya peningkatan kinerja jaringan yang signifikan, ditandai dengan meningkatnya throughput dari 90 Mbps menjadi 105 Mbps, penurunan latency dari 20 ms menjadi 15 ms, serta penurunan packet loss dari 3% menjadi 0,5%. Temuan ini membuktikan bahwa penerapan *firewall* MikroTik mampu meningkatkan keamanan, stabilitas, dan keandalan jaringan, khususnya dalam mendukung kebutuhan operasional perusahaan. Penelitian ini juga merekomendasikan pengembangan lebih lanjut melalui penerapan *Intrusion Detection/Prevention System* (IDS/IPS) serta segmentasi VLAN.

Keywords:

MikroTik Firewall,
Network Security,
Traffic Management,
Cybersecurity,
Network Performance

ABSTRACT

This study aims to analyze the role of firewall implementation on MikroTik RouterOS in improving network security and traffic management at CV. Prima Dinamika Mandiri. The company's network infrastructure consists of an internet service provider router (ISP router), a MikroTik router functioning as the main firewall and gateway, network switches for LAN distribution, multiple access points across work areas, client devices such as laptops, PCs, and servers, as well as shared printers in each office. The firewall was implemented through several configurations, including filtering rules, brute-force protection, Layer 7 filtering, Network Address Translation (NAT), and Quality of Service (QoS), to minimize security threats and optimize network traffic distribution. The evaluation results demonstrate a significant improvement in network performance, as indicated by the increase in throughput from 90 Mbps to 105 Mbps, the reduction of latency from 20 ms to 15 ms, and the decrease in packet loss from 3% to 0.5%. These findings confirm that the implementation of a MikroTik-based firewall enhances network security, stability, and reliability in supporting the company's operational activities. Further development opportunities include the integration of Intrusion Detection and Prevention Systems (IDS/IPS) and VLAN segmentation.

Penulis Korespondensi:

Handrie Noprisson,
Fakultas Teknik dan Informatika,
Universitas Dian Nusantara, Indonesia
Email: handrie.noprisson@dosen.undira.ac.id

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 3, November 2025, hal. 788~793
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

1. PENDAHULUAN

Di era perkembangan teknologi yang semakin pesat, pemanfaatan teknologi informasi telah menjadi bagian mendasar dalam mendukung aktivitas organisasi, industri, pendidikan, hingga pelayanan publik [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]. Infrastruktur jaringan komputer dan internet kini berperan sebagai tulang punggung operasional berbagai sistem informasi, baik untuk pertukaran data, komunikasi, maupun penyediaan layanan digital. Seiring meningkatnya intensitas penggunaan jaringan, kebutuhan terhadap sistem jaringan yang memiliki performa tinggi, stabil, dan aman menjadi semakin penting. Namun, perkembangan teknologi yang cepat juga membawa berbagai ancaman keamanan siber, seperti pencurian data, penyalahgunaan akses, serangan malware, eksploitasi celah keamanan, hingga serangan *Distributed Denial of Service (DDoS)* yang dapat menyebabkan gangguan serius terhadap sistem jaringan [11], [12], [13].

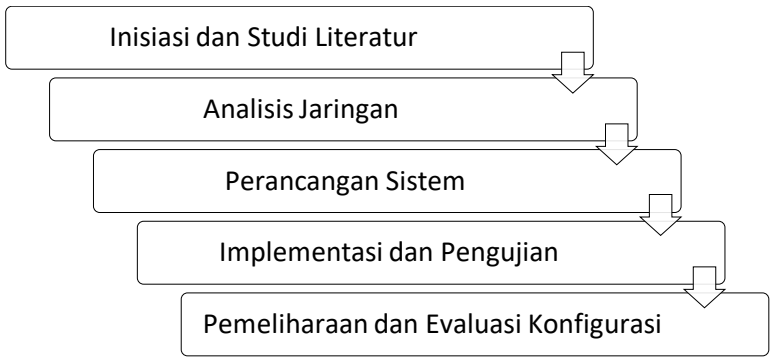
Permasalahan keamanan jaringan tersebut semakin kompleks karena tidak hanya disebabkan oleh serangan dari pihak eksternal, tetapi juga dapat timbul dari kesalahan konfigurasi, kurangnya manajemen trafik, serta lemahnya kebijakan pengendalian akses di dalam jaringan internal. Kondisi ini menunjukkan bahwa pengelolaan trafik jaringan dan keamanan tidak dapat dipisahkan, karena keduanya memiliki peran yang saling berkaitan. Jaringan yang tidak dikelola dengan baik berpotensi mengalami *overload*, *bottleneck*, dan penurunan kualitas layanan, sedangkan jaringan yang tidak dilindungi oleh sistem keamanan yang memadai memiliki risiko tinggi terhadap kebocoran data dan penyusupan pihak yang tidak bertanggung jawab.

Salah satu mekanisme yang banyak digunakan dalam pengamanan jaringan adalah *firewall*. *Firewall* berfungsi sebagai sistem penyaring dan pengendali lalu lintas data yang masuk dan keluar jaringan berdasarkan aturan tertentu, sehingga hanya trafik yang sah dan relevan yang dapat melewati sistem jaringan. MikroTik merupakan salah satu perangkat jaringan yang banyak digunakan karena memiliki fleksibilitas konfigurasi, fitur lengkap, serta biaya yang relatif terjangkau. Fitur *firewall* pada MikroTik memungkinkan administrator jaringan untuk melakukan filtering paket data, *Network Address Translation* (NAT), connection tracking, queue management, hingga proteksi terhadap serangan jaringan [14], [15].

Namun, efektivitas *firewall* MikroTik sangat dipengaruhi oleh desain aturan (*rules*) yang diterapkan. Banyak organisasi yang telah menggunakan MikroTik, tetapi belum menerapkan konfigurasi *firewall* secara optimal, misalnya belum memisahkan trafik berdasarkan kebutuhan layanan, belum membatasi akses port tertentu, atau belum menerapkan mekanisme pencegahan serangan proaktif. Hal ini menyebabkan jaringan tetap berada pada kondisi rentan, meskipun telah menggunakan perangkat pengontrol trafik. Selain itu, belum banyak model implementasi *firewall* yang terdokumentasi sistematis sebagai acuan bagi instansi atau administrator jaringan dalam merancang keamanan yang sesuai dengan kebutuhan operasional.

2. METODE PENELITIAN

Penelitian dilakukan melalui beberapa tahapan. Pertama, dilakukan analisis terhadap kondisi jaringan yang sedang digunakan. Observasi menunjukkan bahwa jaringan belum memiliki firewall yang memadai, seluruh port terbuka, dan tidak terdapat manajemen penggunaan bandwidth. Tahap kedua adalah merancang konfigurasi *firewall* yang sesuai, mencakup NAT, *filtering rules*, proteksi akses *router*, dan Layer 7 *filtering*. Tahap implementasi dilakukan menggunakan perangkat Mikrotik RouterOS melalui aplikasi Winbox. Konfigurasi mencakup pemblokiran paket tidak valid, pemblokiran *port* berbahaya, perlindungan *brute force*, serta penandaan trafik menggunakan fitur *Mangle* untuk kebutuhan QoS. Selanjutnya, dilakukan evaluasi performa jaringan sebelum dan sesudah implementasi dengan parameter latensi, konsumsi bandwidth, dan aktivitas keamanan jaringan dengan tahapan seperti pada **Gambar 1**.

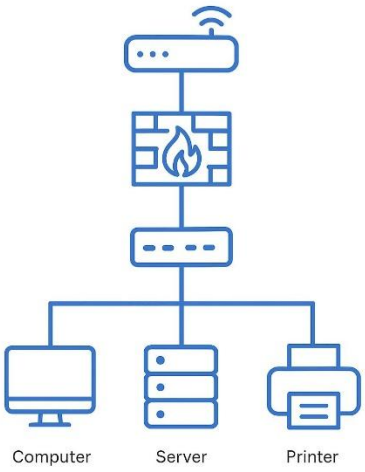


Gambar 1 Tahapan Penelitian

Tahap pertama dimulai dari inisiasi dan studi literatur, yaitu mengidentifikasi kebutuhan keamanan jaringan pada CV. Prima Dinamika Mandiri serta menelaah ancaman yang mungkin muncul dari sisi internal maupun eksternal. Pada tahap ini juga dilakukan analisis risiko terhadap data dan infrastruktur jaringan sehingga diperoleh gambaran awal mengenai tingkat kerentanan sistem yang ada. Hasil kajian ini menjadi dasar dalam penyusunan tujuan serta arah penelitian.
Tahap berikutnya adalah analisis jaringan, yaitu mengevaluasi kondisi arsitektur jaringan yang sedang berjalan serta mengidentifikasi kebutuhan spesifik sistem keamanan. Pada tahap ini ditentukan aturan *firewall*, pola aliran trafik data, serta kebutuhan pengamanan lain yang diperlukan. Analisis ini bertujuan agar rancangan kebijakan keamanan yang disusun benar-benar sesuai dengan kebutuhan operasional perusahaan.
Selanjutnya dilakukan tahap perancangan (*design*), yaitu menyusun rancangan konfigurasi *firewall* MikroTik RouterOS berdasarkan hasil analisis sebelumnya. Tahap ini mencakup penyusunan aturan *filter* paket, pembagian prioritas trafik, pengaturan *bandwidth*, manajemen IP address, serta mekanisme perlindungan tambahan. Rancangan ini juga memperhatikan aspek QoS agar layanan penting tetap memperoleh alokasi bandwidth yang memadai.
Tahap keempat adalah implementasi dan pengujian, yakni menerapkan konfigurasi *firewall* yang telah dirancang pada perangkat MikroTik. Setelah implementasi, dilakukan pengujian melalui simulasi trafik dan potensi serangan untuk memastikan firewall bekerja sesuai harapan. Evaluasi juga melibatkan pengukuran kinerja jaringan menggunakan QoS guna memastikan stabilitas, prioritas layanan, serta pengelolaan bandwidth berjalan optimal. Tahap terakhir adalah pemeliharaan dan evaluasi konfigurasi, yaitu memantau *firewall* berkelanjutan untuk memastikan sistem tetap efektif terhadap ancaman baru. Konfigurasi yang tidak relevan diperbarui atau dihapus agar sistem tetap efisien dan tidak membebani kinerja jaringan.

3. HASIL DAN ANALISIS

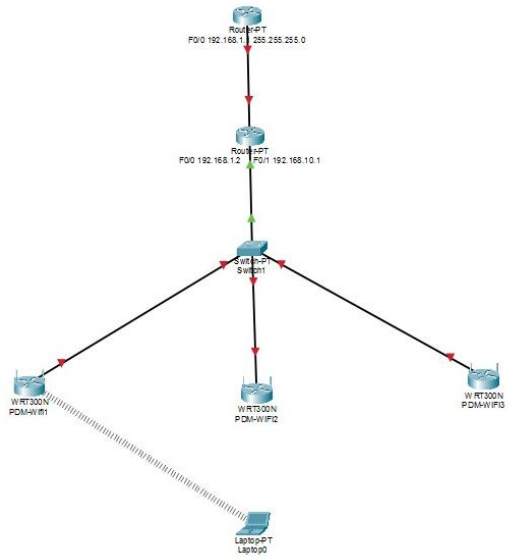
Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan *firewall* pada Mikrotik RouterOS sebagai upaya peningkatan keamanan jaringan dan pengelolaan trafik di CV. Prima Dinamika Mandiri. Permasalahan utama yang dihadapi perusahaan adalah belum optimalnya mekanisme perlindungan jaringan terhadap ancaman eksternal maupun internal, serta tidak meratanya distribusi bandwidth yang berdampak pada stabilitas koneksi. Oleh karena itu, penelitian ini akan memanfaatkan fitur-fitur keamanan pada Mikrotik RouterOS, termasuk *filtering rules*, proteksi *brute force*, Layer 7 *filtering*, *Network Address Translation*, serta *Quality of Service* dengan arsitektur seperti pada **Gambar 2**.



Gambar 2 Konsep Arsitektur Jaringan

Topologi jaringan di CV. Prima Dinamika Mandiri diawali dengan router penyedia layanan internet yang berfungsi sebagai *gateway* menuju jaringan publik, kemudian koneksi diarahkan ke router MikroTik yang bertindak sebagai *firewall*, pengatur jaringan internal, serta pengelola *bandwidth* melalui fitur *Quality of Service*. Dari MikroTik, jaringan didistribusikan melalui *switch* yang ditempatkan di ruang server untuk menghubungkan access point, *server*, dan perangkat lokal lainnya. *Access point* dipasang di beberapa titik strategis agar seluruh area kerja memperoleh akses Wi-Fi tanpa kabel. Perangkat klien yang terhubung berjumlah sekitar 30 unit, termasuk server utama dan server *Accurate*, dengan dukungan printer *sharing* di beberapa ruangan. Seluruh trafik jaringan melewati router MikroTik sehingga dapat difilter, dipantau, dan diatur bandwidth-nya guna menjaga keamanan serta kestabilan koneksi jaringan internal perusahaan dengan arsitektur seperti pada **Gambar 3**.

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 3, November 2025, hal. 788~793
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085



Gambar 3 Pemodelan Jaringan dengan Packtet Tracer

Router pertama yang berada pada bagian paling atas topologi berfungsi sebagai *gateway* jaringan eksternal, yaitu penyedia layanan internet (ISP). Router ini menghubungkan jaringan internal perusahaan dengan jaringan publik sehingga seluruh perangkat di lingkungan CV. Prima Dinamika Mandiri dapat mengakses internet. Perangkat ini tidak dikelola langsung oleh perusahaan, namun hanya berperan sebagai sumber koneksi utama yang kemudian disalurkan ke router berikutnya. Dengan kata lain, router ISP menjadi pintu masuk trafik data dari internet menuju jaringan internal, sekaligus pintu keluar trafik data pengguna menuju internet.
Router MikroTik berada setelah router ISP dan berperan sebagai pusat pengelola jaringan internal. MikroTik direncanakan untuk digunakan sebagai *firewall* guna melindungi jaringan dari akses ilegal dan ancaman eksternal. Selain itu, MikroTik juga menjalankan fungsi NAT (*Network Address Translation*), gateway utama, serta pengatur *Quality of Service* (QoS). Melalui fitur QoS, *bandwidth* dapat dibagi secara adil agar tidak terjadi perebutan kapasitas antar pengguna. Misalnya, ketika satu pengguna melakukan *streaming* video, koneksi pengguna lain tetap stabil. Seluruh trafik internet pada jaringan perusahaan akan melewati MikroTik, sehingga perangkat ini menjadi titik kontrol utama untuk keamanan, monitoring, dan manajemen jaringan dengan beberapa pengaturan sepertu pada **Gambar 4**.

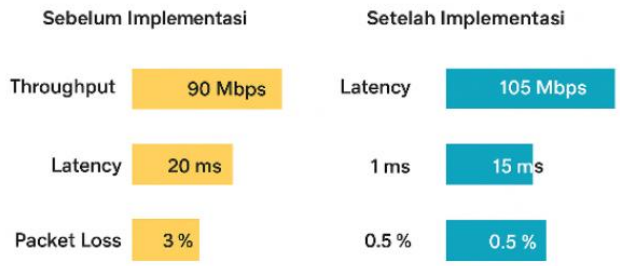
```
/ip firewall nat
add chain=srcnat action=masquerade out-interface=ether1

/ip firewall filter
add chain=input connection-state=invalid action=drop
add chain=forward connection-state=invalid action=drop
add chain=input protocol=top dst-port=22,8291,80 connection-limit=3,32
action=drop
add chain=input protocol=tcp dst-port=23 action=drop
add chain=input protocol=tcp dst-port=445 action=drop

/ip firewall layer7-protocol
add name=sosmed regexp="(*facebook.com|.*tiktok.com|.*ins tagram.com)

/ip firewall mangle
add chain=prerouting protocol=tcp dst-port=4438 action=mark-packet new-packet-
mark=priority_traffic
/queue tree priority_own packet-mark=priority_traffic parent=global download
limit-at=5M max-limit=10M
```

Gambar 4 Implementasi Firewall

Switch ditempatkan di ruang server dan bertugas mendistribusikan jaringan dari router MikroTik ke seluruh perangkat jaringan internal. *Switch* ini menghubungkan berbagai perangkat seperti *access point*, *server*, serta komputer yang membutuhkan akses LAN. Dengan adanya *switch*, lalu lintas data antar perangkat di jaringan internal dapat berjalan lebih terorganisir dan efisien. Switch juga memastikan bahwa komunikasi antar perangkat tetap berjalan optimal tanpa saling mengganggu.

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 3, November 2025, hal. 788~793
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Access point yang digunakan di lapangan adalah perangkat Ubiquiti, namun dalam simulasi pada *Packet Tracer* digambarkan menggunakan perangkat WRT300N. *Access point* berfungsi menyediakan koneksi nirkabel (Wi-Fi) kepada seluruh perangkat pengguna. Titik pemasangan access point tersebar di area strategis, yaitu di depan ruang engineering, dekat ruang meeting 1, 2, dan 3, serta di lantai atas dekat ruang *finance* dan *purchasing*. Penyebaran ini dilakukan agar sinyal Wi-Fi mencakup seluruh ruang kerja, sehingga seluruh karyawan dapat mengakses jaringan tanpa perlu menggunakan kabel LAN.
Perangkat klien yang terhubung ke jaringan terdiri dari sekitar 30-unit laptop/PC, termasuk server utama dan server *Accurate*. Sebagian besar perangkat menggunakan koneksi nirkabel melalui *access point*. Di beberapa ruangan juga terdapat printer yang digunakan bersama (*printer sharing*), seperti dua printer di ruang engineering, satu printer di ruang PPIC, serta beberapa printer di ruang *finance*. Seluruh aktivitas pengguna seperti browsing, pengiriman data, dan akses aplikasi akan melewati router MikroTik, sehingga trafik dapat difilter, dibatasi bandwidth-nya, dan dimonitor. Dengan mekanisme ini, akses ilegal dapat dicegah, penggunaan *bandwidth* tetap terkendali, dan stabilitas jaringan tetap terjaga.
Implementasi *firewall* pada Mikrotik berhasil menutup berbagai celah keamanan yang sebelumnya ada. Hasil menunjukkan penurunan signifikan pada upaya brute force setelah diterapkannya pembatasan akses pada *port* administrasi. *Layer* 7 *filtering* terbukti efektif membatasi akses ke situs non-produktif seperti media sosial dan streaming video. Dari sisi performa, sebelum implementasi *firewall* jaringan perubahan latensi akibat penggunaan *bandwidth* yang tidak terkendali. Latensi turun dan bandwidth untuk aplikasi penting menjadi lebih stabil. Trafik berbahaya seperti invalid packets dan paket dari IP tidak dikenal berhasil diblokir oleh aturan *firewall*. Hasil evaluasi terlihat seperi pada **Gambar 5**.



Gambar 5 Evaluasi Kinerja Jaringan

Throughput meningkat dari 90 Mbps menjadi 105 Mbps, yang berarti kapasitas data yang dapat dikirim setiap detik menjadi lebih besar sehingga akses jaringan terasa lebih cepat. Selain itu, nilai latency turun dari 20 ms menjadi 15 ms, yang menunjukkan bahwa waktu tunda dalam proses pengiriman data semakin kecil sehingga respons jaringan menjadi lebih cepat, khususnya untuk aplikasi *real time*. Penurunan *packet loss* dari 3% menjadi 0,5% juga menggambarkan bahwa semakin sedikit data yang hilang selama proses transmisi, sehingga koneksi menjadi lebih stabil dan andal.

4. KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa implementasi *firewall* pada MikroTik RouterOS memiliki peran yang signifikan dalam meningkatkan keamanan jaringan dan pengelolaan trafik di CV. Prima Dinamika Mandiri. Penerapan filtering rules, proteksi brute force, Layer 7 filtering, NAT, serta *Quality of Service (QoS)* terbukti mampu meminimalkan ancaman keamanan jaringan sekaligus meningkatkan stabilitas dan kualitas koneksi. Infrastruktur jaringan yang terdiri atas router ISP, router MikroTik sebagai firewall dan gateway utama, *switch* jaringan, *access point*, perangkat klien, serta *printer sharing* mendukung penerapan pengamanan dan pengelolaan trafik secara menyeluruh. Secara kinerja, terjadi peningkatan *throughput* dari 90 Mbps menjadi 105 Mbps, penurunan *latency* dari 20 ms menjadi 15 ms, serta penurunan *packet loss* dari 3% menjadi 0,5%. Hal ini menunjukkan bahwa jaringan menjadi lebih cepat, responsif, stabil, dan andal. Ke depan, penguatan keamanan jaringan masih dapat dikembangkan melalui penerapan *Intrusion Detection*/*Prevention System* (IDS/IPS) serta segmentasi VLAN guna memperluas cakupan proteksi dan meningkatkan efisiensi manajemen jaringan. Dengan demikian, model implementasi *firewall* MikroTik ini dapat menjadi acuan strategis dalam membangun sistem jaringan yang aman.

UCAPAN TERIMA KASIH

Terima kasih kepada Lembaga Riset dan Pengabdian Kepada Masyarakat Universitas Dian Nusantara yang telah memberikan dukungan pendanaan sehingga penelitian ini dapat terlaksana dengan baik. Penulis juga menyampaikan terima kasih yang sebesar-besarnya kepada seluruh staf dan karyawan CV. Prima Dinamika

Mandiri yang telah memberikan izin, kesempatan, serta fasilitas yang diperlukan sehingga penulis dapat melakukan pengamatan jaringan secara langsung.

REFERENSI

[1] D. Ramayanti, S. D. Asri, and L. Lionie, "Implementasi Model Arsitektur VGG16 dan MobileNetV2 Untuk Klasifikasi Citra Kupu-Kupu," *JSAI (Journal Sci. Appl. Informatics)*, vol. 5, no. 3, pp. 182–187, 2022.

[2] S. D. Asri, I. Jaya, A. Buono, and S. H. Wijaya, "Fish Detection in Seagrass Ecosystem using Masked-Otsu in HSV Color Space," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 12, 2022.

[3] H. Noprisson and Budiyarti, "Aplikasi Manajemen Pemeliharan Produk Perangkat Lunak," *J. Sci. Appl. Informatics*, vol. 1, no. 2, pp. 41–45, 2018.

[4] V. Ayumi, "Studi Pendahuluan: Pengembangan Aplikasi m-BCARE Untuk Pasien Penderita Kanker Payudara," *JUSIBI (Jurnal Sist. Inf. dan E-Bisnis)*, vol. 3, no. 1, pp. 26–33, 2021.

[5] A. Ratnasari, D. Fitrianah, and W. H. Haji, "BPTrends Redesign Methodology (BPRM) for the Development Disaster Management Prevention Information System," in *Proceedings of the 2020 2nd Asia Pacific Information Technology Conference*, 2020, pp. 113–117.

[6] N. Ani, H. Noprisson, and N. M. Ali, "Measuring usability and purchase intention for online travel booking: A case study," *Int. Rev. Appl. Sci. Eng.*, vol. 10, no. 2, pp. 165–171, 2019.

[7] H. Noprisson, "Exploring e-Tourism : Technology and Human Factors," *Int. J. Sci. Res. Sci. Eng. Technol.*, pp. 169–177, Sep. 2021, doi: 10.32628/IJSRSET207540.

[8] M. Mishbah, D. I. Sensuse, and H. Noprisson, "Information system implementation in smart cities based on types, region, sub-area," *2017 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2017 - Proc.*, vol. 2018-Janua, pp. 155–161, 2017, doi: 10.1109/ICITSI.2017.8267935.

[9] D. I. Sensuse, P. Prima, E. Cahyaningsih, and H. Noprisson, "Knowledge management practices in e-Government," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, IEEE Xplore, 2017.

[10] H. Noprisson, "Enterprise 2.0: Identifying Factors for Technology Adoption Based on Technological, Organizational, Human and Social Dimensions," *JSAI (Journal Sci. Appl. Informatics)*, vol. 6, no. 1, pp. 59–64, 2023.

[11] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol. 22, no. 3, p. 1094, 2022.

[12] A. Singh and B. B. Gupta, "Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," *Int. J. Semant. Web Inf. Syst.*, vol. 18, no. 1, pp. 1–43, 2022.

[13] U. Islam *et al.*, "Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models," *Sustainability*, vol. 14, no. 14, p. 8374, 2022.

[14] Y. Xu, B. Du, and L. Zhang, "Self-attention context network: Addressing the threat of adversarial attacks for hyperspectral image classification," *IEEE Trans. Image Process.*, vol. 30, pp. 8671–8685, 2021.

[15] J. Ye, X. D. C. De Carnavalet, L. Zhao, M. Zhang, L. Wu, and W. Zhang, "Exposed by default: A security analysis of home router default settings," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 2024, pp. 63–79.