REVIEW: PERBANDINGAN SOLUSI KEAMANAN SKALABILITAS DALAM NDN

Adhitya Fathana[1)] **I Putu Sugi Almantara**[2)]
Program Studi Teknologi Informasi [1) 2)]
Universitas Udayana, Badung, Bali [1) 2)]
adhityafathana236@gmail.com [(1)] sugialmantara@unud.ac.id [2)]

ABSTRACT

This research reviews the performance and security aspects of NDN with a focus on scalability solutions. NDN, as part of ICN, offers a unique approach with data (object) naming at its core, differing from the location-based orientation of TCP/IP. The implementation of RBAC and ABAC is evaluated through the SLR method. The research highlights the positive performance of NDN in addressing loop issues, improving responsiveness, and ensuring good throughput. NDN's security is enhanced through data encryption, authentication, and digital signatures. Threat prevention and security evolution demand adaptive access control solutions. Proposed solutions include the use of advanced security technologies, robust encryption implementation, expanded authentication, and artificial intelligence integration for proactive responses to security threats.

Keywords*: ABAC, NDN, RBAC, Security, SLR.*

ABSTRAK

Penelitian ini mengulas kinerja dan keamanan NDN dengan fokus pada solusi terhadap masalah skalabilitas. NDN, sebagai bagian dari ICN, menawarkan pendekatan unik dengan penamaan data (objek) sebagai inti, berbeda dengan pendekatan TCP/IP yang berorientasi pada alamat lokasi. Penerapan RBAC dan ABAC dievaluasi melalui metode SLR. Hasil penelitian menyoroti kinerja positif NDN dalam menangani masalah *loop*, meningkatkan waktu tanggap, dan throughput yang baik. Keamanan NDN ditingkatkan melalui enkripsi data, otentikasi, dan tanda tangan digital. Pencegahan ancaman dan evolusi keamanan menuntut solusi kontrol akses yang adaptif. Solusi yang diusulkan mencakup penggunaan teknologi keamanan canggih, penerapan enkripsi yang kuat, otentikasi yang diperluas, dan integrasi kecerdasan buatan untuk respons proaktif terhadap ancaman keamanan.

Kata Kunci: ABAC, NDN, RBAC, Security, SLR.

PENDAHULUAN

Informasi dianggap sebagai elemen krusial dalam struktur organisasi. Itulah sebabnya sebagian besar terfokus pada keamanan informasi untuk melindungi data organisasi dari ancaman baik yang berasal dari internal maupun eksternal. Kontrol akses yang digunakan untuk menjaga kerahasiaan informasi dari akses yang tidak sah dan juga menentukan hak akses yang diberikan atau dicabut kepada pengguna atau sistem [1]. Di era informasi dapat diakses dari mana saja, terutama melalui internet, penting untuk mempertimbangkan skalabilitas keamanan untuk memastikan bahwa sistem dan data tetap terlindungi dengan efektif. Untuk mengatasi tantangan yang signifikan yang timbul akibat pertumbuhan pesat pengguna, jaringan NDN juga melibatkan mekanisme *routing* yang telah terbukti memiliki peran krusial dalam. Dalam memastikan bahwa pesan-pesan menarik dapat menemukan jalur untuk *content request*. Saat ini, mekanisme *routing* IP adalah teknik yang telah matang, terbukti dengan menghubungkan seluruh entitas internet di seluruh dunia. Dengan penggunaan routing yang hampir tanpa upaya, sebuah entitas dapat terhubung dengan entitas lain, meskipun entitas yang terlibat mungkin berada dalam jarak geografis yang berjauhan [2].

Saat ini, mekanisme *routing* IP telah menjadi teknik matang yang menghubungkan entitas di seluruh dunia dengan hampir tanpa upaya. Namun, dalam konteks keamanan dan skalabilitas, NDN menawarkan pendekatan

yang berbeda. NDN adalah salah satu arsitektur *Information-Centric Networking* (ICN) yang paling khas. Konsep dasarnya berfokus pada penamaan data (objek), berbeda dengan pendekatan TCP/IP yang lebih berorientasi pada alamat lokasi. NDN membawa keunggulan seperti *caching* dalam jaringan, keamanan berbasis data, pengiriman multi-jalur, dan mobilitas [3]. Pada penelitian ini akan membahas mengenai *literature review* perbandingan solusi keamanan skalabilitas dalam NDN. Dengan mempertimbangkan aspek atau keunggulan metode yang disajikan oleh NDN pada jurnal yang diacu, diharapkan mendapatkan solusi keamanan skalabilitas menggunakan NDN.

METODE PENELITIAN

Metode penelitian *literature review* yang diaplikasikan dalam penelitian ini bertujuan untuk membandingkan solusi terhadap masalah skalabilitas pada *Named Data Networking* (NDN) dengan evaluasi dan perbandingan antara model *Role Based Access Control* (RBAC) dan *Attribute Based Access Control* (ABAC). Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk memastikan keakuratan dan obyektivitas dalam mengumpulkan, mengevaluasi, dan menganalisis literature terkait. Berikut merupakan langkah-langkah utama dalam metode penelitian ini.

Penetapan Tujuan Penelitian

Menetapkan tujuan penelitian untuk membandingkan solusi terhadap masalah skalabilitas di NDN dan melakukan evaluasi serta perbandingan antara model RBAC dan ABAC.

Pemilihan Kriteria Inklusi

Identifikasi kriteria inklusi dan eksklusi untuk menentukan literatur yang relevan dengan fokus penelitian. Kriteria ini membantu memilih studi yang memenuhi persyaratan penelitian.

Pencarian Literatur

Menggunakan SLR sebagai metode pencarian literatur. Pencarian dilakukan secara sistematis dengan kata kunci yang relevan, memastikan kelengkapan sumber informasi yang akan dieva**l**uasi lanjut.

Seleksi dan Pengumpulan Data

Melibatkan pemilihan sumber literatur yang sesuai dengan kriteria inklusi dan eksklusi. Data yang relevan diekstrak dari literatur yang terpilih untuk kemudian dianalisis lebih

Evaluasi Kualitas Literatur

Menilai kualitas setiap literatur yang terpilih, termasuk metodologi penelitian, bukti yang disajikan, dan relevansi dengan tujuan penelitian. Evaluasi ini membantu menentukan keandalan informasi yang diambil.

Analisis Perbandingan

Menganalisis temuan dari literatur yang memperbandingkan solusi terhadap masalah skalabilitas pada NDN, Selanjutnya, dilakukan analisis terhadap literatur yang mengevaluasi serta membandingkan model RBAC dan ABAC.

Sintesis Temuan

Sintesiskan temuan dari kedua fokus penelitian untuk memberikan pemahaman yang komprehensif mengenai hubungan antara solusi terhadap masalah skalabilitas di NDN dan perbandingan antara model RBAC dan ABAC.

Penyusunan Laporan

Susun laporan *literature review* dengan jelas, termasuk pendahuluan yang menjelaskan konteks penelitian, metode yang digunakan, temuan utama, dan kesimpulan yang merinci temuan serta implikasinya dalam konteks penelitian.

STUDI LITERATUR

Bagian ini membahas temuan hasil dari SLR yang difokuskan pada perbandingan sebelumnya, dengan tujuan memahami aspek-aspek tertentu dalam konteks NDN dan mengevaluasi perbandingan antara model RBAC dan ABAC.

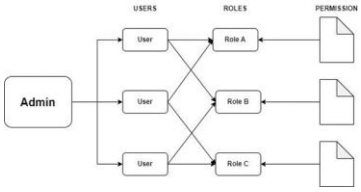
Named Data Network (NDN)

Named Data Networking (NDN) pertama kali diajukan oleh Van Jacobson, yang terinspirasi oleh peningkatan signifikan penggunaan internet hingga mencapai titik kritis. Fokusnya adalah memanfaatkan internet secara *end-to-*

end untuk distribusi dan pengambilan konten. NDN sendiri mengusulkan perkembangan dalam arsitektur IP yang memungkinkan paket-paket diberi nama sebagai objek daripada titik akhir komunikasi. Ini merubah terminologi IP di mana paket-paket yang dikirim ke alamat tujuan diidentifikasi berdasarkan nama yang diberikan. Sesuai dengan namanya, dalam paket NDN, nama dapat mencakup berbagai hal, mulai dari titik akhir hingga jenis data umum seperti film, buku, atau bahkan tindakan tertentu. Melalui spesifikasinya, NDN dapat mengatasi keterbatasan penamaan IP yang ada dalam arsitektur IP [4].

Role-Based Access Control (RBAC)

RBAC memudahkan pengguna dalam mengakses aplikasi dan sumber daya dengan struktur yang terorganisir. Kelebihan RBAC tidak hanya berfokus pada manajemen akses pengguna, tetapi juga memberikan kontribusi dalam mengatasi tantangan keamanan dan skalabilitas pada NDN. Penerapan RBAC dalam NDN tidak hanya mempermudah administrasi, tetapi juga memberikan solusi efektif terhadap pertumbuhan kompleksitas sistem NDN dengan memusatkan kontrol akses melalui peran-peran yang ditentukan, meningkatkan keamanan dan skalabilitas [1].

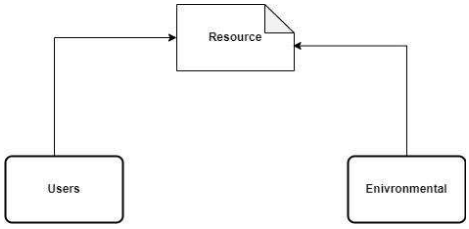


Gambar 1. Diagram RBAC

Hirarki RBAC ditetapkan oleh *administrator*, yang memungkinkan penetapan izin yang berbeda untuk setiap *roles*. Dengan adanya *roles* yang telah ditetapkan, *users* dapat mengakses *file* dan data di jaringan sesuai dengan wewenang yang dimiliki, mengurangi potensi akses tidak sah terhadap informasi dan aplikasi yang bersifat sensitif.

Attribute-Based Access Control (ABAC)

ABAC adalah model kontrol akses yang fokus pada permintaan subjek untuk menjalankan operasi pada objek berdasarkan atribut seperti waktu dan lokasi. ABAC tidak hanya memberikan kontrol akses yang granular dan dapat diperbarui secara dinamis, tetapi juga berkontribusi positif dalam meningkatkan keamanan dan mengatasi tantangan skalabilitas pada NDN. Dengan memanfaatkan ABAC, implementasi kontrol akses dalam NDN menjadi lebih terstruktur, efisien, dan skalabel [1].



Gambar 2. Diagram ABAC

Dalam hirarki ABAC, izin diatur berdasarkan berbagai atribut yang bekerja secara bersama-sama untuk menjaga keamanan dokumen. Dalam kosep ini, elemen-elemen seperti subyek, objek, dan operasi bekerja secara terkoordinasi untuk menentukan akses.

HASIL DAN PEMBAHASAN

Berdasarkan pendekatan SLR mengenai keamanan dalam NDN didapat sejumlah temuan. Adapun temuan-temuan yang didapatkan berdasarkan literatur yang ditemukan akan disampaikan pada sub bab berikut.

Kinerja NDN

Penelitian yang dilakukan oleh Sri Astuti, dkk membahas mengenai kinerja NDN sebagai jaringan internet masa depan yang data *centric* dan adaptif. Dengan menggunakan strategi *forwarding* penelitian ini mencoba mengatasi masalah *loop* dalam *routing* dengan memanfaatkan *Loop Free Inport-Dependent* (LFID) *protocol*. Hasilnya menunjukkan bahwa strategi *forwarding* nilai *delay* yang sangat baik, mengindikasikan potensi optimalisasi kinerja NDN melalui pilihan *forwarding* yang tepat [5]. Penelitian berikutnya dilakukan oleh Peiter Solarso Pasaribu, dkk membahas mengenai integrasi NDN dengan *Software Defined Network* (SDN) dengan tujuan agar *routing* tidak bergantung pada *Network Flooding* dari NDN, melainkan

menjadi tanggung jawab SDN. Hasilnya menunjukkan bahwa untuk waktu tanggap yang lebih rendah dalam skenario topologi kompleks, NDN lebih baik, namun dalam topologi linear, NDN-SDN lebih baik. Demikian juga, dalam hal *throughput* dan penggunaan CPU, kombinasi NDN-SDN cenderung lebih unggul daripada NDN sendiri [6]. Penelitian selanjutnya dilakukan oleh Yaoqing Liu, dkk membahas mengenai evaluasi kinerja NDN yang merupakan salah satu arsitektur internet masa depan yang menjanjikan. NDN dapat digunakan untuk mengatasi kemacetan lalu lintas dan memberi prioritas pada pesan kritis baik pada jaringan kabel maupun nirkabel. Pengukuran kinerja NDN dalam berbagai pengaturan jaringan nyata dan melakukan perbandingan langsung dengan pendekatan berbasis TCP/IP [7].

Berdasarkan beberapa penelitian NDN menunjukkan kinerja yang positif sebagai arsitektur internet masa depan. *Strategi forwarding* dapat mengatasi masalah *loop* dalam *routing*, dan hasilnya menunjukkan nilai delay yang sangat baik, hal ini menunjukkan bahwa NDN dapat dioptimalkan dengan baik melalui pilihan *forwarding* yang tepat [5]. Integrasi NDN dengan SDN juga dianggap unggul, meskipun NDN lebih baik dalam waktu tanggap pada skenario topologi kompleks, kombinasi NDN-SDN menjadi lebih unggul dalam topologi linear serta cenderung lebih baik dalam *througput* dan penggunaan CPU [6]. Selanjutnya NDN sebagai arsitektur yang menjanjikan dengan kemampuan mengatasi kemacetan lalu lintas dan memberi prioritas pada pesan kritis di berbagai jenis jaringan, menunjukkan kompetensi dan potensi implementasi NDN dalam berbagai situasi jaringan [7].

Skalabilitas Jaringan dan Efisien

Skalabilitas jaringan dan efisiensi dimaksud untuk memastikan kemampuan jaringan NDN untuk menangani pertumbuhan skala besar dan mengelola permintaan data yang tinggi tanpa mengorbankan kinerja. Penelitian yang dilakukan oleh Tody A, dkk membahas mengenai NDN yang mengusung paradigma yang berbeda dari jaringan internet konvesional dan memberikan perubahan mendasar dalam implementasi komunikasi data di internet. Skalabilitas menjadi fokus utama, yaitu kemampuan jaringan untuk mengatasi masalah yang muncul seiring dengan bertambahnya entitas di internet. Tingginya intensitas beban jaringan dengan jumlah node dan konten yang besar menciptakan beban besar pada mekanisme internet. Untuk mengatasinya, mekanisme NDN harus efisien sehingga dengan pertumbuhan cepat jaringan, kinerja NDN tidak dikorbankan [2]. Penelitian selanjutnya dilakukan oleh Yu Zhang, dkk membahas mengenai identifikasi dampak perubahan arsitektural node IP menuju NDN terhadap *routing* dan *forwarding* dalam jaringan. Berdasarkan penelitian yang dilakukan didapat argumen bahwa pertemuan pada data membuka dimensi baru dalam ruang solusi untuk skalabilitas jaringan [8]. Penelitian selanjutnya dilakukan oleh Ahmad Tantoni, dkk membahas mengenai perbaikan akses jaringan internet dan sistem informasi pada salah satu perguruan tinggi swasta yang mengkhususkan diri dalam ilmu komputer. Penelitian ini mengidentifikasi permasalahan mengenai akses lambat yang disebabkan oleh infrastruktur jaringan komputer, dengan melakukan desain ulang jaringan komputer maka skalabilitas civitas kampus akan meningkat. Hasilnya adalah desain antara *layout* gedung kampus baru dan *blueprint* infrastruktur jaringan komputer yang konkret sehingga meningkatkan kinerja jaringan dan manfaat jangan panjang bagi pengelola teknologi [9].

Keamanan Data dan Integrasi

Keamanan data dan integrasi pada NDN dapat dilakukan dengan implementasi enkrpisi data, otentikasi, dan tanda tangan digital. Implementasi ini dimaksud untuk melindungi kerahasiaan dan memastikan integraitas data dalam perpindahan pada jaringan NDN. Penelitian pertama dilakukan oleh Elídio Tomas da Silva, dkk menjelaskan bahwa bagian keamanan pada konteks NDN mencakup aspek-aspek seperti routing, chacing, dan keamanan data bawaan. Dengan *routing*, NDN memberikan cara yang lebih aman dalam mengelola alamat data daripada model konvensional berbasis IP. Selain itu, *caching*

memungkinkan penyimpanan data secara terdistribusi di *node* jaringan, menungkatkan efisiensi, dan mengurangi ketergantungan pada sumber pusat. Keamanan data bawaan NDN menciptakan lingkungan yang lebih aman untuk pertukaran informasi dalam VANET yang dinamis, memastikan bahwa data yang dikirim tetap terlindungi dan terotentikasi [10]. Keamanan NDN dapat diintegrasikan pada beberapa bidang. Pada penelitian Zakaria Sabir menjelaskan penerapan NDN dalam lingkungan kendaraan membawa dampak positif terhadap keamanan data. Keamanan data dalam konteks ini mencakup perlindungan informasi yang dikirim dan diterima dalam jaringan kendaraan. Dengan menggunakan NDN, yang berfokus pada komunikasi berbasis data, integritas dan otentikasi data dapat ditingkankan. NDN juga memanfaatkan keamanan bawaan melalui penamaan data yang unik dan penanganan keamanan yang terintegrasi. Secara keseluruhan, integrasi NDN dalam jaringan kendaraan menghadirkan solusi yang lebih tangkas dan aman dalaman manajemen data, memastikan keamanan informasi yang dikomunikasikan pada lingkungan yang sering berubah dan dinamis [11]. Selain keamanan di darat, NDN juga mampu melakukan keamanan pada laut. Penelitian yang dilakukan oleh Vasudeva A R membahas mengenai integrasi NDN dalam *Underwater Wireless Sensor Network* (UWSN) membawa dampak positif terhadap perlindungan data di lingkungan bawah air yang terbatas. NDN dapat mengatasi tantangan keamanan unik dalam komunikasi UWSN, termasuk melindungi data dari potensi ancaman dan manipulasi. Dengan fokus pada komunikasi berbasis data, NDN membentuk lapisan keamanan yang dapat meningkatkan integritas dan otentikasi data [12].

Pencegahan Ancaman dan Evolusi Keamanan

Pencegahan ancaman dan evolusi keamanan melibatkan mekanisme pencegahan serangan dan ancaman, serta memastikan bahwa solusi keamanan dapat berkembang seiring dengan perkembangan teknologi dan kebutuhan jaringan. Penelitian yang dilakukan oleh Yuen Fei membahas mengenai solusi kontrol akses baru yang dapat beradaptasi baik untuk lingkingan tertutup maupun terbuka. Upaya yang dapat dilakukan adalah dengan memperkenalkan logika BAN yang disesuaikan. Logika ini dapat digunakan untuk menggambarkan keyakinan pihak-pihak terkait dalam prosedur solusi kontrol akses yang diidealkan. Dengan memformulasikan tujuan keamanan dan pstulat logis, dilakukan analisis terhadap prosedur tersebut. Hasil analisis digunakan untuk memodifikasi solusi kontrol akses dengan tujuan membuatnya lebih aman. Penelitian juga memasukkan skenario serangan *man-in-the-middle* ke dalam solusi kontrol akses, sehingga dapat diidentifikasi dan dicari solusi untuk potensi ketidakamanannya. Dengan demikian, penelitian ini memberikan evolusi pada aspek keamanan solusi kontrol akses dalam konteks NDN, membantu mengidentifikasi dan mencegah potensi ancaman keamanan yang mungkin timbul [13]. Penelitian yang dilakukan oleh Philipp Moll membahas mengenai pengembangan protokol *Sync* dalam arsitektur NDN. Analisis menyatakan bahwa setiap protokol *Sync* dapat dicirikan oleh keputusan desainnya terhadap tiga komponen dasar, yaitu representasi *namespace dataset*, *encoding namespace* untuk berbagi, dan mekanisme pemberitahuan perubahan. Selama evolusi data NDN, dapat diamati bahwa terdapat dua atau tiga jenis pilihan desain untuk setiap komponen tersebut. Dalam pengembangan protokol *Sync*, hubungan anatara transportasi dan penamaan aplikasi, implikasi *encoding namespace* terhadap skalabilitas grup *Sync*, dan kebutuhan fundamental akan *Sync* Intrest *multicast* [14].

Perbandingan RBAC dan ABAC

RBAC dan ABAC menjadi krusial dalam pengaturan keamanan informasi. RBAC memberikan akses berdasarkan peran, dengan struktur hierarki peran yang memberikan keteroganisasian yang baik, cocok untuk organisasi besar. Di sisi lain, ABAC menawarkan akses yang didasarkan pada atribut atau karakteristik pengguna, sumber daya, dan lingkungan, seperti peran, lokasi geografis, dan waktu akses, memberikan fleksibiltas tinggi sesuai untuk lingkungan yang dinamis [15]. Selanjutnya penelitian yang

dilakukan oleh Marcel Danilescu membahas mengenai perbedaan antara RBAC dan ABAC yang terletak pada pendekatan dasar kontrol akses. RBAC berfokus pada hierarki peran pengguna di dalam organisasi, dengan hak akses yang ditentukan oleh peran yang dimainkan. Sebaliknya, ABAC memusatkan perhatian pada atribut atau karakteristik pengguna, sumber daya, dan lingkungan, memungkinkan hak akses yang lebih fleksibel berdasarkan kombinasi atribut [16]. Berdasarkan penelitian yang dilakukan oleh Kritika Soni dan Suresh Kumar mengenai perbandingan model *security private cloud* menggunakan RBAC dan ABAC, RBAC lebih menonjol dalam kesederhanaan dan struktur yang terorganisasi, lebih efisiensi dalam manajemen izin. ABAC sendiri dianggap lebih fleksibel dan adaptif, lebih terfokus pada akses kontrol pengguna yang lebih presisi [17].

SIMPULAN

Penelitian terkait NDN menyoroti kinerja yang positif, terutama dalam penanganan masalah *loop*, peningkatan waktu tanggap, dan *throughput* yang baik. Strategi *forwarding* yang efektif dan integrasi dengan SDN memberikan keuntungan, terutama dalam mengelola *routing* pada topologi kompleks dan *linear*. Meskipun demikian, keamanan data dalam konteks NDN menjadi fokus penting.

Pentingnya keamanan data pada NDN tercermin dalam implementasi enkripsi data, otentikasi, dan tanda tangan digital. Meskipun NDN memiliki fitur keamanan bawaan seperti routing yang lebih aman dan *caching* terdistribusi, langkah-langkah tambahan diperlukan untuk melindungi data dan memastikan integritasnya. Pencegahan ancaman dan evolusi keamanan menjadi aspek vital, dan penelitian menunjukkan upaya dalam mengembangkan solusi kontrol akses yang adaptif terhadap lingkungan dinamis dan kompleks.

Solusi yang dapat diimplementasikan untuk meningkatkan keamanan pada NDN melibatkan penggunaan teknologi keamanan yang lebih canggih dan adaptif. Penerapan metode enkripsi yang lebih kuat, otentikasi yang diperluas, dan pengembangan solusi kontrol akses yang dinamis dapat menjadi langkah kunci. Selain itu, pemanfaatan kecerdasan buatan dalam mendeteksi dan merespons terhadap ancaman keamanan dapat meningkatkan respon proaktif jaringan. Dengan mengintegrasikan strategi ini, NDN dapat memberikan kinerja optimal tanpa mengabaikan aspek keamanan yang krusial.

DAFTAR PUSTAKA

[1] Muhammad umar Aftab, Zhiguang Qin, Zakria, Safeer Ali, Pirah, Jalaluddin Khan. (2018). The Evaluation and Comparative Analysis of Role Based Access Control and Attribute Based Access Control Model. 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) (pp. 35 - 39). Chengdu, China: IEEE.

[2] Tody Ariefianto Wibowo, N. R. (2019). Named Data Network (NDN) Scalability Problem. 2019 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob) (pp. 112 - 118). Bali, Indonesia: IEEE.

[3] Zhiwei Yan, Yong-Jin Park, Yu-Beng Leau, Lee Ren-Ting, Rosilah Hassan. (2020). Hybrid Network Mobility Support in Named Data Networking. 2020 International Conference on Information Networking (ICOIN) (pp. 16 - 19). Barcelona, Spain: IEEE.

[4] Ratna Mayasari, Nana Rachmana Syambas. (2020). Machine Learning on Named Data Network: A survey Routing and Forwarding Strategy. 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA) (pp. 1 - 5). Bandung, Indonesia: IEEE.

[5] Sri Astuti, Tody Ariefianto Wibowo, Ratna Mayasari, Ibnu Asror, Gregorius Pradana Satriawan. (2020). Klasifikasi Data Delay dengan LFID Strategi Forwarding menggunakan Machine Learning untuk Memaksimalkan Kinerja Jaringan NDN (Named Data Network). Vol. 14 No. 2 (2020): Jurnal Computech &

Bisnis (e-Journal), 115-122.

[6] Peiter Solarso Pasaribu, Leanna Vidya Yovita, Sofia Naning Hertiana. (2022). Analisis Perbandingan Kinerja Routing Statis Pada Named Data Networking Berbasis Software Defined Networking Dan Routing Nlsr Pada NDN Tradisional. e-Proceeding of Engineering : Vol.8, No.6 Desember 2022, 2691-2700.

[7] Yaoqing Liu, Anthony Dowling, Lauren Huie. (2020). Benchmarking Network Performance in Named Data Networking (NDN). 2020 29th Wireless and Optical Communications Conference (WOCC) (pp. 1 - 6). Newark, NJ, USA: IEEE.

[8] Yu Zhang, Zhongda Xia, Alexander Afanasyev, Lixia Zhang. (2019). A Note on Routing Scalability in Named Data Networking. 2019 IEEE International Conference on Communications Workshops (ICC Workshops). Shanghai, China: IEEE.

[9] Ahmad Tantoni, Arief Setyanto, Eko Pramono. (2018). ANALISIS DAN PERANCANGAN BLUEPRINT INFRASTRUKTUR JARINGAN KOMPUTER UNTUK MENDUKUNG IMPLEMENTASI SISTEM INFORMASI PADA STMIK LOMBOK. Jurnal Informasi Interaktif Vol.3 No.1 Januari 2018, 67 - 76.

[10] Elídio Tomás Silva, António Luís Duarte Costa, Joaquim Melo Henriques Macedo. (2022). On the realization of VANET using named data networking: On improvement of VANET using NDN-based routing, caching, and security. International Journal of Communication Systems Volume 35, Issue 18, 1-48.

[11] Zakaria Sabir, Aouatif Amine. (2021). Connected Vehicles using NDN: Security Concerns and Remaining Challenges. 2021 7th International Conference on Optimization and Applications (ICOA) (pp. 1 - 6). Wolfenbüttel, Germany: IEEE.

[12] Prajisha C, Vasudevan A R. (2020). Security Challenges in NDN Based Underwater Wireless Sensor Networks: An Overview. Proceedings of the 2nd International Conference on IoT, Social, Mobile, Analytics & Cloud in Computational Vision & Bio-Engineering (ISMAC-CVB 2020) (pp. 210-223). India: SSRN.

[13] Yuan Fei, Huibiao Zhu, Phan Cong Vinh . (2020). Security Analysis of the Access Control Solution of NDN Using BAN Logic. Mobile Networks and Applications.

[14] Philipp Moll, Varun Patil, Lan Wang, Lixia Zhang . (2022). SoK: The evolution of distributed dataset synchronization solutions in NDN. ICN '22: Proceedings of the 9th ACM Conference on Information-Centric Networking, 33–44.

[15] Gunjan Batra, Vijayalakshmi Atluri, Jaideep Vaidya, Shamik Sural. (2019). Deploying ABAC policies using RBAC systems. Journal of Computer Security, 483–506.

[16] Marcel Danilescu. (2021). Comparative Study of Access Control Methods in Enterprise Information Systems, Based on RBAC, ABAC, and TBAC policies. Performance and Risks in the European Economy, 177-184.

[17] Kritika Soni, Suresh Kumar. (2019). Comparison of RBAC and ABAC Security Models for Private Cloud. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 584 - 587). Faridabad, India: IEEE