Journal of Artificial Intelligence and Software Engineering
Vol. 5, No. 4, Desember 2025, pp. 1340~1347
E-ISSN: 2777-001X, DOI: 10.30811/jaise.v5i4.7083

Explanatory Case Study on the Implementation of Quantum Communication Protocols in Enhancing the Security of Industrial Internet of Things Networks

Dara Sawitri
Jurusan Teknik Elektro, Fakultas Teknik Dan Komputer, Universitas Harapan Medan, Jl. H.M Joni no.70 C Medan. 20217, Indonesia

Informasi Artikel

Diterima : 05 Juni 2025
Revisi : 02 Oktober 2025
Publikasi : 31 Desember 2025

Kata Kunci:

Internet of Things (IoT);
Quantum communication;
Data security;
Industrial IoT;
communication protocols:

ABSTRAK

Internet of Things (IoT) masih menghadapi persoalan mendasar terkait keamanan komunikasi, yang dipicu oleh keterbatasan sumber daya perangkat serta sifatnya yang tersebar secara luas. Penerapan komunikasi kuantum dipandang sebagai terobosan strategis dalam memperkuat perlindungan data melalui mekanisme enkripsi berbasis prinsip kuantum. Penelitian ini diarahkan pada analisis implementasi sekaligus adaptasi protokol komunikasi kuantum dalam ekosistem IoT industri dengan tujuan meningkatkan tingkat keamanan pertukaran data. Temuan menunjukkan bahwa keberhasilan penerapan sangat dipengaruhi oleh dua faktor utama, yaitu kesesuaian teknis perangkat dan pengelolaan aspek organisasional, meliputi koordinasi lintas unit serta resistensi terhadap perubahan. Kebaruan kajian ini terletak pada orientasinya terhadap penerapan nyata protokol komunikasi kuantum dalam lingkungan industri, yang sebelumnya lebih dominan dikaji melalui pendekatan teoretis atau berbasis simulasi. Dengan mengintegrasikan dimensi teknis dan manajerial, penelitian ini memberikan kontribusi terhadap pemahaman komprehensif mengenai mekanisme adaptasi protokol kuantum, sekaligus menawarkan rekomendasi praktis bagi pengembangan strategi keamanan komunikasi yang aplikatif dan berkelanjutan.

The Internet of Things (IoT) continues to face fundamental challenges in communication security, primarily due to the limited resources of devices and their highly distributed nature. The integration of quantum communication is considered a strategic breakthrough to strengthen data protection through encryption mechanisms based on quantum principles. This research is directed toward analyzing the implementation and adaptation of quantum communication protocols within industrial IoT ecosystems, with the aim of enhancing the security of data exchange. The findings indicate that the success of implementation is strongly influenced by two major factors: the technical compatibility of devices and the management of organizational aspects, including cross-unit coordination and resistance to change. The novelty of this study lies in its focus on real-world implementation of quantum communication protocols in industrial environments, which have previously been examined predominantly through theoretical or simulation-based approaches. By integrating both technical and managerial dimensions, this research contributes to a comprehensive understanding of adaptation mechanisms for quantum protocols while providing practical recommendations for the development of more applicable and sustainable communication security strategies.

Penulis Koresponden

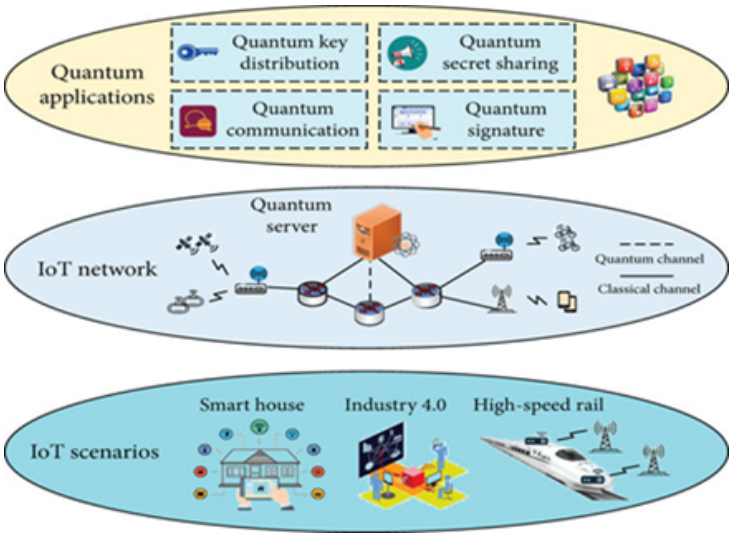
Email: dara.sawitri.24@gmail.com

Cara sitasi IEEE:

D. Sawitri, "Explanatory Case Study on the Implementation of Quantum Communication Protocols in Enhancing the Security of Industrial Internet of Things Networks" *Journal of Artificial Intelligence and Software Engineering (J-AISE)*, vol. 5, no. 4, pp. 1340–1347, Desember 2025, doi:10.30811/jaise.v5i4.7083

1. PENDAHULUAN

Perkembangan teknologi Internet of Things (IoT) telah merevolusi cara perangkat terhubung dan berkomunikasi, membuka peluang besar di berbagai sektor seperti industri, kesehatan, dan transportasi. Namun, peningkatan konektivitas juga membawa tantangan yang signifikan, terutama dalam hal keamanan komunikasi data yang rentan terhadap berbagai ancaman siber [1]. Di tengah semakin kompleksnya jaringan IoT, teknologi komunikasi kuantum telah muncul sebagai solusi potensial untuk meningkatkan keamanan dengan prinsip enkripsi berbasis mekanika kuantum yang secara teoritis tidak dapat ditembus oleh metode klasik. Masalah keamanan komunikasi IoT menjadi semakin penting mengingat sifat perangkat IoT yang sering kali memiliki sumber daya terbatas dan tersebar di lingkungan yang *heterogen*, membuat keamanan tradisional kurang efektif [2]. Kebutuhan akan protokol komunikasi yang tidak hanya kuat secara *kriptografi* tetapi juga adaptif terhadap karakteristik IoT yang unik menuntut pendekatan baru yang dapat mengatasi tantangan ini secara *holistik*. Terhadap latar belakang ini, pemahaman yang mendalam tentang bagaimana protokol komunikasi kuantum dapat diterapkan dan diadaptasi dalam konteks IoT yang nyata menjadi sangat penting[3].
.



Gambar 1. Kerangka kerja IoT berbasis kuantum.
Sumber Gang Liu, Jingyuan Han, Yi Zhou, Tao Liu, dan Jian Chen, 2022

Penelitian ini diarahkan untuk menyelidiki secara kontekstual dan mendalam dinamika implementasi komunikasi kuantum dalam jaringan IoT industri sebagai upaya menjembatani kesenjangan antara teori dan praktik di lapangan[4]. Kasus yang menjadi fokus penelitian ini adalah implementasi protokol komunikasi kuantum dalam jaringan IoT di sebuah perusahaan *manufaktur*. Perusahaan ini telah mengadopsi teknologi komunikasi kuantum sebagai langkah strategis untuk meningkatkan keamanan data dalam proses produksi dan pengelolaan informasi penting. Jaringan IoT yang digunakan mencakup berbagai perangkat *sensor, aktuator*, dan sistem kontrol yang tersebar di berbagai lini produksi dan gudang [5]. Konteks ini unik karena menghadapi tantangan teknis dan organisasi yang kompleks, seperti kebutuhan untuk mengintegrasikan perangkat lama dengan teknologi kuantum baru, sumber daya perangkat IoT yang terbatas, dan adaptasi personel teknis dan manajerial terhadap teknologi canggih ini. Situasi ini mencerminkan realitas implementasi teknologi *inovatif*

dalam lingkungan industri yang dinamis dan penuh tekanan secara operasional [6], [7]. Meskipun teknologi komunikasi kuantum telah banyak dipelajari secara teoritis dan simulasi, hanya sedikit penelitian yang secara *komprehensif* mengkaji bagaimana protokol ini diadaptasi dan dijalankan dalam jaringan IoT industri seperti dalam kasus ini. Dengan mempertimbangkan dinamika tersebut, penelitian ini ditujukan untuk menyelidiki secara mendalam konteks implementasi komunikasi kuantum dalam jaringan IoT di perusahaan manufaktur sebagai representasi tantangan dan peluang di lapangan.

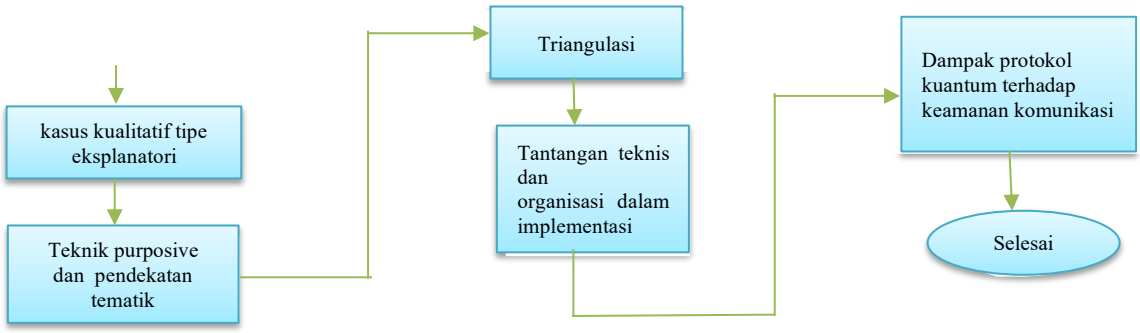
Perkembangan teknologi komunikasi kuantum dalam beberapa tahun terakhir telah menempatkannya sebagai salah satu terobosan penting dalam meningkatkan keamanan data. Hal ini menjadi semakin signifikan ketika dikaitkan dengan jaringan Internet of Things (IoT), yang pada sektor industri modern berfungsi sebagai tulang punggung proses produksi, distribusi, hingga manajemen rantai pasok. Penerapan IoT di perusahaan manufaktur melibatkan ribuan perangkat sensor, aktuator, dan sistem kontrol yang secara simultan menghasilkan serta mengolah data dalam jumlah besar. Kondisi ini menimbulkan kerentanan yang semakin kompleks, karena arus informasi yang masif sangat rawan terhadap gangguan dan ancaman siber. Oleh karena itu, komunikasi kuantum dipandang sebagai solusi strategis yang mampu memperkuat lapisan keamanan data sekaligus menjawab kebutuhan industri terhadap sistem yang lebih andal.

Namun, kenyataan di lapangan menunjukkan bahwa adopsi komunikasi kuantum dalam jaringan IoT industri tidaklah sederhana. Integrasi perangkat lama dengan teknologi baru, keterbatasan daya dan kapasitas komputasi perangkat IoT, serta kebutuhan akan interoperabilitas menimbulkan tantangan teknis yang cukup besar. Di sisi lain, aspek organisasional juga tidak kalah krusial. Kesiapan sumber daya manusia, mekanisme manajerial, hingga besarnya biaya investasi menciptakan hambatan tersendiri dalam proses implementasi. Situasi ini mencerminkan bahwa keberhasilan penerapan komunikasi kuantum di sektor industri tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan organisasi untuk menavigasi perubahan secara adaptif. Dengan demikian, kompleksitas implementasi komunikasi kuantum dalam IoT industri[8].

Merupakan fenomena multidimensional yang menuntut kajian mendalam dari berbagai perspektif. Sejauh ini, literatur yang ada masih cenderung menitikberatkan pada aspek teoritis dan simulasi laboratorium, sementara kajian empiris terkait penerapan nyata komunikasi kuantum di jaringan IoT industri masih sangat terbatas. Kesenjangan inilah yang melatar belakangi pentingnya penelitian ini, yang diarahkan untuk menelaah secara kontekstual proses implementasi komunikasi kuantum dalam lingkungan manufaktur. Penelitian ini bertujuan untuk mengungkap dinamika tantangan teknis dan organisasional, strategi adaptasi yang diterapkan perusahaan, serta implikasi praktisnya terhadap keberlanjutan operasional dan keamanan data. Dengan mengintegrasikan analisis teknis dan manajerial, penelitian ini menawarkan kontribusi ganda: secara teoretis memperluas pemahaman mengenai adopsi teknologi kuantum dalam IoT industri, dan secara praktis memberikan rekomendasi strategi yang lebih aplikatif dan berorientasi pada keberlanjutan.

2. METODE

Penelitian ini menggunakan pendekatan studi kasus *kualitatif* dengan tipe *eksplanatori* untuk mengeksplorasi secara mendalam implementasi protokol komunikasi kuantum pada jaringan *Internet of Things* (IoT) di lingkungan industri [9]. Studi kasus dipilih karena memungkinkan pemahaman *kontekstual* tentang fenomena kompleks yang melibatkan interaksi teknologi, organisasi, dan manusia dalam situasi nyata. Kasus yang dipelajari adalah jaringan IoT di perusahaan *manufaktur* yang telah mengadopsi protokol komunikasi kuantum untuk meningkatkan keamanan data[10]. Unit analisis utama adalah proses implementasi protokol kuantum dan dinamika teknis dan organisasi yang menyertainya dalam konteks operasional perusahaan. Informan penelitian terdiri dari para ahli teknologi informasi, manajer proyek, dan operator sistem yang terlibat langsung dalam implementasi teknologi kuantum di jaringan IoT. Teknik *purposive* sampling digunakan untuk memilih partisipan yang memiliki peran kunci dan pengetahuan mendalam terkait proses implementasi. Data dikumpulkan melalui analisis dokumen. Observasi mendukung pemahaman tentang konteks fisik dan operasional implementasi protokol kuantum. Data dianalisis menggunakan pendekatan *tematik* melalui pengkodean terbuka, kategorisasi, dan pengembangan tema utama yang mencerminkan proses adaptasi, tantangan, dan dampak teknologi kuantum pada keamanan komunikasi.*Triangulasi* data dilakukan dengan menggabungkan informasi dari wawancara, observasi, dan dokumen untuk memperkuat keabsahan temuan. Validasi tambahan dilakukan melalui *member checking* dengan beberapa informan kunci untuk memastikan bahwa interpretasi data akurat dan *representatif*. Seluruh proses pengumpulan dan analisis data dilakukan dengan prinsip *chain of evidence*, yang memungkinkan penelusuran hubungan antara data mentah, pengkodean, tema, dan kesimpulan akhir. Hal ini memastikan transparansi dan *kredibilitas* hasil penelitian.



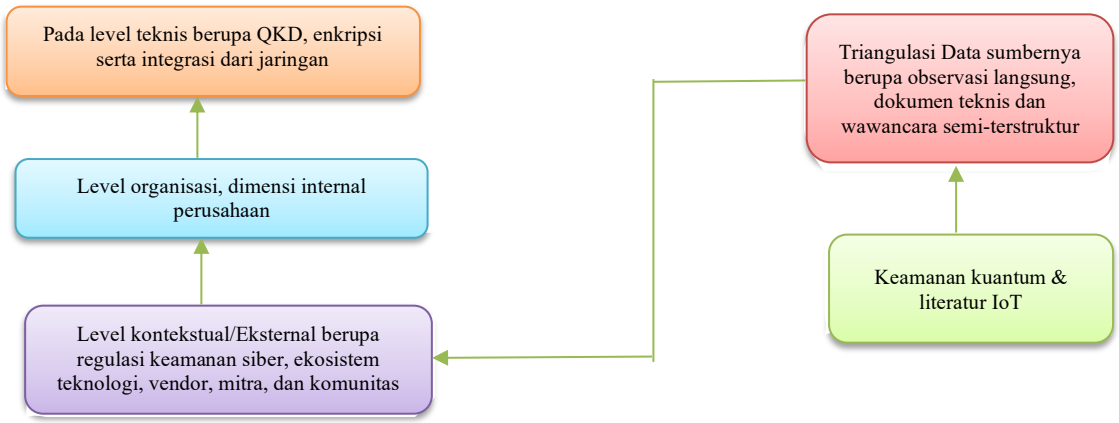
Gambar 2 Diagram Alur Penelitian

3. HASIL DAN PEMBAHASAN

Studi ini menemukan bahwa penerapan protokol komunikasi kuantum pada jaringan IoT industri memerlukan proses adaptasi yang kompleks. Perangkat IoT yang memiliki sumber daya terbatas harus disesuaikan dengan protokol kuantum yang biasanya memerlukan infrastruktur dan proses komputasi yang intensif [11]. Seorang informan teknis menyatakan, Proses ini melibatkan kolaborasi lintas tim teknis untuk memastikan kompatibilitas dan efisiensi, yang juga menunjukkan perlunya koordinasi yang kuat antara unit pengembangan.

3.1 Kasus kualitatif tipe eksplanatori

Penelitian ini menggunakan studi kasus kualitatif tipe eksplanatori untuk menelaah implementasi protokol komunikasi kuantum dalam meningkatkan keamanan IoT industri. Pendekatan ini dipilih karena mampu menjelaskan mengapa dan bagaimana teknologi tersebut diadopsi, sekaligus menghubungkan teori keamanan kuantum dengan praktik di lapangan. Pada Gambar 3 berikut ini visual bagan kerangka analisis kasus eksplanatori adalah sebagai berikut :



Gambar 3 Visual bagan kerangka analisis kasus eksplanatori

Penjelasan Gambar 3 Visual bagan kerangka analisis kasus eksplanatori adalah visualisasi bagan kerangka analisis kasus eksplanatori ini merepresentasikan keterkaitan antara tiga lapisan analisis, yaitu teknis, organisasional, dan kontekstual, yang kemudian dipadukan melalui strategi triangulasi data. Seluruh lapisan tersebut dianalisis dengan merujuk pada landasan teori keamanan kuantum serta literatur IoT, sehingga menghasilkan kerangka penjelasan yang utuh mengenai dinamika implementasi protokol komunikasi kuantum dalam meningkatkan keamanan jaringan IoT industri. .kerangka analisis penelitian ini dibangun atas tiga tingkatan utama, yakni teknis, organisasi/manajerial, serta kontekstual. Pada level teknis, fokus diarahkan pada implementasi protokol komunikasi kuantum melalui *Quantum Key Distribution (QKD)*, pengelolaan kunci enkripsi, dan integrasi dengan infrastruktur komunikasi klasik. Level organisasi/manajerial meninjau faktor internal perusahaan seperti kebijakan keamanan, kesiapan sumber daya manusia, serta aspek investasi, sedangkan level kontekstual menelaah pengaruh regulasi, standar industri, dan dukungan ekosistem teknologi.

Ketiga lapisan ini saling melengkapi untuk menjelaskan dinamika penerapan komunikasi kuantum dalam memperkuat keamanan jaringan IoT industri. Analisis tersebut diperkuat melalui penerapan triangulasi data yang melibatkan observasi langsung, kajian dokumen teknis, dan wawancara semi-terstruktur. Selanjutnya, hasil temuan diperdalam dengan landasan teori keamanan kuantum serta literatur IoT, sehingga menghasilkan penjelasan eksplanatif yang komprehensif mengenai sejauh mana protokol komunikasi kuantum dapat, atau belum dapat dijadikan sebagai solusi strategis bagi keamanan jangka panjang IoT industri.

3.2 Teknik purposive, pendekatan tematik dan triangulasi

Dalam penelitian ini, informan dipilih melalui teknik purposive, yaitu penentuan partisipan secara selektif berdasarkan relevansi dan keterlibatan individu atau pihak yang dipilih secara sengaja karena dianggap paling relevan dengan topik penelitian, misalnya :

a. **Level teknis** mencakup individu seperti insinyur jaringan, pakar IoT, maupun tim teknologi informasi yang secara langsung menangani pengelolaan serta perlindungan sistem.
b. **Level manajerial** meliputi peran manajer keamanan informasi, pimpinan divisi TI, hingga pengambil keputusan strategis dalam organisasi.
c. **Level kontekstual** mencakup aktor eksternal, antara lain regulator, konsultan industri, serta pihak lain yang berhubungan dengan penerapan standar keamanan dan kebijakan regulatif.

Data yang terkumpul kemudian dianalisis menggunakan pendekatan tematik untuk mengidentifikasi pola, kategori, dan tema utama dari berbagai sumber data. Sinergi kedua metode tersebut memungkinkan penelitian eksplanatori memberikan penjelasan yang komprehensif mengenai alasan dan cara implementasi protokol komunikasi kuantum dalam mendukung keamanan IoT industri.

Teknik purposive diterapkan untuk menentukan informan penelitian berdasarkan relevansi dan keterlibatan langsung terhadap fenomena yang dikaji, yang terdiri atas tiga kategori: teknis (insinyur jaringan, pakar IoT, tim TI), manajerial (manajer keamanan informasi, kepala divisi TI, pengambil kebijakan), serta kontekstual (regulator, konsultan industri, dan pihak eksternal terkait regulasi).

Analisis data dilakukan melalui pendekatan tematik dengan tahapan pengodean, pengelompokan, dan pembentukan tema, sehingga memungkinkan identifikasi pola hubungan antar-dimensi teknis, organisasional, dan kontekstual dalam menjelaskan implementasi protokol komunikasi kuantum pada keamanan IoT industri.

Triangulasi digunakan dalam studi kasus eksplanatori ini untuk memperkuat validitas data melalui kombinasi sumber, metode, dan teori. Melibatkan informan dari level teknis, manajerial, dan kontekstual, serta data dari wawancara, observasi, dan dokumen, pendekatan ini memberikan pemahaman menyeluruh tentang penerapan protokol komunikasi kuantum bagi keamanan IoT industri.

3.3 Tantangan Teknis dan Organisasi dalam Implementasi

Hambatan teknis utama yang teridentifikasi meliputi keterbatasan perangkat keras, *interoperabilitas* antara perangkat lama dan baru, serta kebutuhan akan pelatihan sumber daya manusia. Selain itu, terdapat tantangan organisasi terkait dengan penolakan terhadap perubahan dan kurangnya pemahaman mendalam tentang teknologi kuantum. Hal ini menunjukkan bahwa faktor manusia dan organisasi memainkan peran penting dalam keberhasilan adopsi teknologi baru. Temuan utama terkait keamanan menunjukkan bahwa protokol komunikasi kuantum secara signifikan meningkatkan ketahanan jaringan terhadap ancaman siber seperti penyadapan dan serangan *spoofing*. Data observasi menunjukkan bahwa implementasi Distribusi Kunci *Kuantum (QKD*) memungkinkan *enkripsi* kunci yang tidak dapat dipecahkan oleh komputer klasik[12].

Table 1 Integration of IoT and Quantum Communication Protocols in Network Security

Aspect	Key Findings	Implications/Recommendations
Quantum Protocol Adaptation	IoT devices must be optimized to be compatible with quantum protocols; cross-team collaboration is essential.	The need for technical adjustments and cross-functional coordination for successful implementation of quantum technologies.
Technical And Organizational Challenges	Limitations of legacy devices, resistance to change, and lack of training are major barriers.	The need for intensive training and effective change management to support the adoption of quantum technologies.
Communications Security Impact	The implementation of quantum protocols enhances security with	Increase IoT network resilience against cyber attacks and data leaks.

	impenetrable encryption and interception detection.	
Practical Implications	Managing technical and managerial collaboration is key to managing quantum technologies in IoT.	Training strategies and resource support must be optimized to accelerate the adoption of new technologies.
Study Limitations	The study is still limited to one case of industrial IoT network and is contextual.	Further, multi-case studies are needed to increase the generalizability of the results.
Research Recommendations	Cross-sector comparative studies, quantitative approaches, and longitudinal analyses are recommended.	Expanding the understanding of quantum protocol adaptation and its effectiveness across various IoT contexts.

3.4 Dampak Protokol Kuantum terhadap Keamanan Komunikasi

Pengembangan protokol komunikasi kuantum menghadirkan perubahan signifikan dalam upaya peningkatan keamanan komunikasi, terutama dalam konteks *Internet of Things* (IoT) yang menghadapi tantangan kompleks dari perangkat berdaya rendah dan jaringan heterogen. Ditekankan bahwa perangkat IoT berdaya rendah dalam jaringan 5G menghadapi ancaman keamanan dan privasi yang serius karena keterbatasan sumber daya yang membatasi penerapan teknik enkripsi konvensional. Protokol kuantum, seperti *Quantum*), diusulkan sebagai solusi yang dapat menyediakan enkripsi yang secara teoritis tidak dapat dipecahkan, meningkatkan ketahanan komunikasi terhadap serangan siber [12], [13]. Dalam laporan IoT *Analytics,* keamanan merupakan salah satu tantangan utama IoT, di mana protokol komunikasi kuantum dipandang sebagai teknologi yang berpotensi mengatasi kelemahan keamanan tradisional dengan menawarkan perlindungan berdasarkan prinsip fisika kuantum, bukan hanya algoritma matematika[14]. Tren ini mengidentifikasi komunikasi kuantum sebagai salah satu dari 10 perkembangan teknologi paling relevan dalam IoT, yang mampu mengubah paradigma keamanan data dalam skala besar, terutama dalam aplikasi industri dan infrastruktur penting[15]. Dalam sebuah studi tentang sistem komunikasi asli kuantum, dinyatakan bahwa penerapan protokol kuantum membawa transformasi paradigma keamanan komunikasi dari enkripsi klasik ke enkripsi berbasis mekanika kuantum, dengan potensi untuk menghilangkan risiko penyadapan yang tidak terdeteksi[12], [16]. Namun, mereka juga mencatat tantangan teknis dan integrasi, terutama dalam jaringan IoT yang beragam dan dinamis. Tinjauan komprehensif tren komunikasi kuantum, menyoroti bahwa protokol kuantum tidak hanya meningkatkan keamanan komunikasi tetapi juga menciptakan kebutuhan untuk inovasi dalam desain perangkat keras dan manajemen sumber daya, terutama dalam aplikasi IoT [17]. Mereka menekankan pentingnya penelitian lebih lanjut untuk mengatasi keterbatasan implementasi di dunia nyata dan memperkuat *interoperabilitas* protokol kuantum dengan teknologi IoT yang ada. Secara keseluruhan, literatur saat ini mengonfirmasi bahwa protokol komunikasi kuantum memiliki dampak besar dalam memperkuat keamanan komunikasi IoT dengan mengurangi risiko kebocoran data dan serangan siber, tetapi implementasinya masih menghadapi tantangan teknis, sumber daya, dan integrasi yang perlu ditangani secara menyeluruh dalam konteks aplikasi nyata[3], [18].

3.5 Pembahasan

Hasil penelitian ini mengungkap bahwa keberhasilan penerapan protokol komunikasi kuantum pada jaringan IoT industri sangat bergantung pada proses adaptasi teknis yang cermat, pengelolaan tantangan organisasi, dan penguatan keamanan melalui mekanisme *enkripsi* kuantum[12], [19]. Adanya tantangan tersebut menunjukkan bahwa selain aspek teknologi, faktor manusia dan organisasi merupakan kunci utama dalam penerapan komunikasi aman berbasis IoT kuantum. Hasil penelitian mengungkap bahwa penerapan protokol komunikasi kuantum pada jaringan IoT industri sangat bergantung pada proses adaptasi teknis yang cermat, pengelolaan tantangan organisasi, dan penguatan keamanan melalui mekanisme *enkripsi* kuantum[20]. Adanya tantangan tersebut menunjukkan bahwa selain aspek teknologi, faktor manusia dan organisasi merupakan kunci utama dalam penerapan komunikasi aman berbasis IoT kuantum. Jaringan IoT industri dipengaruhi oleh kebutuhan adaptasi teknis yang intensif dan tantangan organisasi yang signifikan. Temuan ini menunjukkan bahwa keberhasilan implementasi teknologi ini tidak hanya bergantung pada kecanggihan teknis, tetapi juga pada koordinasi lintas tim dan manajemen *resistensi* terhadap perubahan di tingkat

organisasi. Studi ini menjelaskan secara konkret bagaimana para pelaku di lapangan, termasuk insinyur dan manajer proyek, menavigasi keterbatasan perangkat keras dan kurangnya pengalaman teknis melalui kolaborasi dan pembelajaran berkelanjutan. Temuan ini menunjukkan dinamika adaptif yang belum banyak disorot dalam studi sebelumnya yang lebih berfokus pada aspek teknologi murni dan simulasi, sehingga memberikan kontribusi baru untuk memahami penerapan teknologi kuantum dalam lingkungan operasional nyata. Selain itu, hasil studi ini konsisten dengan konsep implementasi *adaptif* dan teori manajemen perubahan, di mana teknologi baru sering kali memerlukan penyesuaian struktural dan perilaku organisasi agar dapat berfungsi secara optimal. Tidak seperti studi sebelumnya yang lebih menekankan pada aspek teknis, kasus ini menyoroti pentingnya komunikasi informal dan dukungan antara para pelaku sebagai mekanisme penting dalam mengatasi hambatan implementasi.

4. KESIMPULAN

Hasil studi kasus eksplanatori ini menegaskan bahwa penerapan protokol komunikasi kuantum memberikan kontribusi yang substansial terhadap peningkatan keamanan jaringan IoT industri, khususnya melalui mekanisme distribusi kunci kuantum, autentikasi perangkat, serta integrasi dengan infrastruktur komunikasi klasik. Pada level teknis, protokol kuantum terbukti mampu mengatasi keterbatasan kriptografi konvensional, sedangkan pada level manajerial keberhasilan implementasi sangat ditentukan oleh kesiapan sumber daya manusia, strategi kebijakan, serta alokasi investasi yang memadai. Selanjutnya, pada level kontekstual, dukungan regulasi, kesesuaian standar industri, dan dinamika ekosistem teknologi menjadi faktor eksternal yang turut menentukan keberlanjutan adopsi. Dengan mempertautkan ketiga level analisis tersebut, penelitian ini menghasilkan pemahaman yang komprehensif mengenai alasan serta mekanisme implementasi protokol komunikasi kuantum dalam konteks IoT industri. Temuan ini sekaligus menegaskan bahwa keberhasilan adopsi tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga sangat dipengaruhi oleh kapasitas organisasi dan dukungan lingkungan eksternal. Oleh karena itu, protokol komunikasi kuantum dapat diposisikan sebagai alternatif strategis jangka panjang dalam menjawab tantangan keamanan IoT industri, meskipun penerapannya masih dihadapkan pada berbagai hambatan teknis, manajerial, maupun regulatif yang menuntut solusi berkesinambungan.

REFERENSI

[1] D. Sawitri, “Big Data Challenges And Opportunities In The Development Of Digital Technology,” *Informatika dan Sains*, vol. 14, no. 02, p. 2024, doi: 10.58471/infosains.v14i02.

[2] M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchain-based architecture for secure smart home for lightweight IoT,” *Inf Process Manag*, vol. 58, no. 3, 2021, doi: 10.1016/j.ipm.2020.102482.

[3] G. Liu, J. Han, Y. Zhou, T. Liu, and J. Chen, “QSLT: A Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks,” *Wirel Commun Mob Comput*, vol. 2022, no. 1, 2022, doi: 10.1155/2022/4809210.

[4] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, “Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities,” *Inf Process Manag*, vol. 58, no. 4, 2021, doi: 10.1016/j.ipm.2021.102549.

[5] K. Lakshmanna, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalafand, and A. K. Nanda, “Improved Metaheuristic-Driven Energy-Aware Cluster-Based Routing Scheme for IoT-Assisted Wireless Sensor Networks,” *Sustainability (Switzerland)*, vol. 14, no. 13, 2022, doi: 10.3390/su14137712.

[6] O. Friha, M. A. Ferrag, M. Benbouzid, T. Berghout, B. Kantarci, and K.-K. R. Choo, “2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT,” *Comput Secur*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103097.

[7] D. Sawitri, “Artificial Intelligence for a Digital Technology Smart Society in the Era of Society 5.0,” *Journal of Artificial Intelligence and Software Engineering (J-AISE)*, vol. 5, no. 1, p. 135, Mar. 2025, doi: 10.30811/jaise.v5i1.6441.

[8] N. M. Abdulkareem, S. R. M. Zeebaree, M. A. M. Sadeeq, D. M. Ahmed, A. S. Sami, and R. R. Zebari, “IoT and Cloud Computing Issues, Challenges and Opportunities: A Review,” *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, 2021, doi: 10.48161/qaj.v1n2a36.

[9] C. Shao, Y. Yang, S. Juneja, and T. GSeetharam, “IoT data visualization for business intelligence in corporate finance,” *Inf Process Manag*, vol. 59, no. 1, 2022, doi: 10.1016/j.ipm.2021.102736.

[10] X. Wang, “Pursuing the fundamental limits for quantum communication,” *IEEE Trans Inf Theory*, vol. 67, no. 7, pp. 4524–4532, 2021, doi: 10.1109/TIT.2021.3068818.

[11] M. Allaix, Y. Lu, Y. Yao, T. Pllaha, C. Hollanti, and S. A. Jafar, "N-Sum Box: An Abstraction for Linear Computation over Many-to-One Quantum Networks," *IEEE Trans Inf Theory*, vol. 71, no. 2, pp. 1121–1139, 2025, doi: 10.1109/TIT.2024.3514921.
[12] K. Yao, W. O. Krawec, and J. Zhu, "Quantum Sampling for Finite Key Rates in High Dimensional Quantum Cryptography," *IEEE Trans Inf Theory*, vol. 68, no. 5, pp. 3144–3163, 2022, doi: 10.1109/TIT.2022.3141874.
[13] O. D. Okey *et al.*, "Quantum Key Distribution Protocol Selector Based on Machine Learning for Next-Generation Networks," *Sustainability (Switzerland)*, vol. 14, no. 23, 2022, doi: 10.3390/su142315901.
[14] A. M. Kelly, M. Darienzo, T.-C. Wei, and D. Schneble, "Quantum information science and technology professional learning for secondary science, technology, engineering, and mathematics teachers," *Phys Rev Phys Educ Res*, vol. 20, no. 2, 2024, doi: 10.1103/PhysRevPhysEducRes.20.020154.
[15] A. Minbaleev, S. Zenin, and K. Evsikov, "Prospects for Legal Regulation of Quantum Communication," *BRICS Law Journal*, vol. 11, no. 2, pp. 11–54, 2024, doi: 10.21684/2412-2343-2024-11-2-11-54.
[16] M. Rezai and J. A. Salehi, "Quantum CDMA Communication Systems," *IEEE Trans Inf Theory*, vol. 67, no. 8, pp. 5526–5547, 2021, doi: 10.1109/TIT.2021.3087959.
[17] L. Belli *et al.*, "IoT-enabled smart sustainable cities: Challenges and approaches," *Smart Cities*, vol. 3, no. 3, pp. 1039–1071, 2020, doi: 10.3390/smartcities3030052.
[18] M. Frey, I. Bjelakovic, J. Notzel, and S. Stanczak, "Semantic Security With Infinite-Dimensional Quantum Eavesdropping Channel," *IEEE Trans Inf Theory*, vol. 71, no. 4, pp. 2662–2697, 2025, doi: 10.1109/TIT.2025.3531250.
[19] J. Yoon, "The Rise of Quantum Technology and Its Implications for National Security," *Korean Journal of Defense Analysis*, vol. 36, no. 1, pp. 25–48, 2024, doi: 10.22883/kjda.2024.36.1.002.
[20] M. Krelina, "The Prospect of Quantum Technologies in Space for Defence and Security," *Space Policy*, vol. 65, 2023, doi: 10.1016/j.spacepol.2023.101563.