ASEFBA: Advanced Studies in Economic, Finance and Banking
eISSN: XXXX-XXXX
**Vol 1, No 1, April 2025**
DOI: https://doi.org/10.123456/asefba.v1i1.xxxx

# Digitalisasi Perbankan dan Ancaman Keamanan Siber: Tantangan dan Strategi Mitigasi Risiko Operasional

**Romy Setiawan[1], Rahmadsyah[2]**
*[12]Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda*
Corresponding author: romysetiawan@gmail.com

**Abstrak**

Artikel ini bertujuan untuk menganalisis tantangan yang dihadapi oleh industri perbankan dalam menghadapi digitalisasi dan ancaman keamanan siber, serta mengidentifikasi strategi mitigasi risiko operasional yang efektif. Metode penelitian yang digunakan adalah studi literatur komprehensif yang mengkaji berbagai publikasi ilmiah, laporan industri, dan studi kasus terkait digitalisasi perbankan, keamanan siber, dan manajemen risiko. Hasil penelitian menunjukkan bahwa digitalisasi perbankan membawa berbagai manfaat, seperti peningkatan efisiensi, aksesibilitas, dan pengalaman pelanggan. Namun, digitalisasi juga meningkatkan eksposur terhadap ancaman keamanan siber, termasuk serangan *malware*, *phishing*, serangan *denial-of-service* (DoS), dan kebocoran data. Penelitian mengidentifikasi beberapa strategi mitigasi risiko yang efektif, meliputi penerapan kerangka kerja keamanan yang komprehensif, investasi dalam teknologi keamanan siber canggih, pengembangan kesadaran keamanan siber, dan kolaborasi antara lembaga keuangan, pemerintah, dan sektor swasta. Kesimpulan dari penelitian ini adalah bahwa digitalisasi perbankan memerlukan pendekatan proaktif dan holistik terhadap keamanan siber. Lembaga keuangan harus terus berinvestasi dalam teknologi dan praktik terbaik untuk mengurangi risiko operasional dan melindungi aset serta data pelanggan.

**Kata kunci**: *Digitalisasi Perbankan, Keamanan Siber, Risiko Operasional, Mitigasi Risiko, Fintech*

## Pendahuluan

Industri perbankan telah mengalami transformasi signifikan dalam beberapa dekade terakhir, didorong oleh kemajuan teknologi dan digitalisasi. Perubahan ini telah mengubah cara lembaga keuangan beroperasi, berinteraksi dengan pelanggan, dan menyediakan layanan keuangan. Digitalisasi perbankan, yang mencakup penggunaan teknologi digital untuk mengoptimalkan proses bisnis dan memberikan layanan kepada pelanggan, menawarkan banyak manfaat, termasuk peningkatan efisiensi operasional, pengurangan biaya, peningkatan aksesibilitas layanan, dan peningkatan pengalaman pelanggan (Dwivedi et al., 2023).

Namun, digitalisasi perbankan juga menimbulkan tantangan signifikan, terutama terkait dengan keamanan siber. Peningkatan ketergantungan pada teknologi digital telah memperluas permukaan serangan bagi pelaku kejahatan siber. Serangan siber terhadap lembaga keuangan dapat mengakibatkan kerugian finansial yang besar, kerusakan reputasi, hilangnya kepercayaan pelanggan, dan bahkan gangguan sistemik pada stabilitas keuangan (Eling & Schnell, 2016). Ancaman keamanan siber terus

• Submitted: 10-01-2025 • Revisi: 20-02-2025 • Diterima: 04-03-2025

berkembang dalam kompleksitas dan frekuensi, dengan serangan yang semakin canggih dan sulit dideteksi.

Masalah penelitian yang mendasar adalah bagaimana menyeimbangkan manfaat digitalisasi perbankan dengan risiko keamanan siber yang meningkat. Kesenjangan dalam penelitian ini terletak pada kebutuhan untuk mengembangkan strategi mitigasi risiko operasional yang komprehensif dan efektif yang dapat melindungi lembaga keuangan dari ancaman siber yang terus berkembang. Tujuan dari penelitian ini adalah untuk mengidentifikasi tantangan utama yang dihadapi oleh industri perbankan dalam menghadapi digitalisasi dan ancaman keamanan siber, serta untuk mengembangkan strategi mitigasi risiko yang efektif.

Digitalisasi perbankan telah mengubah lanskap industri keuangan secara fundamental. Teknologi digital, seperti internet, komputasi awan, kecerdasan buatan (AI), dan teknologi seluler, telah memungkinkan lembaga keuangan untuk menawarkan layanan yang lebih cepat, lebih efisien, dan lebih mudah diakses (Allen et al., 2021; Koohang et al., 2023). Perkembangan ini telah mendorong munculnya berbagai inovasi, termasuk perbankan seluler, pembayaran digital, pinjaman *online*, dan layanan keuangan berbasis *blockchain* (Wang et al., 2018; Abou Jaoude & Saadé, 2019).

Transformasi digital dalam perbankan tidak hanya tentang mengadopsi teknologi baru, tetapi juga tentang mengubah model bisnis dan budaya organisasi. Tronvoll et al. (2020) berpendapat bahwa digitalisasi memerlukan pergeseran strategis, termasuk perubahan dari perencanaan ke penemuan, dari kelangkaan ke kelimpahan, dan dari hierarki ke kemitraan. Perusahaan harus berinvestasi dalam kapabilitas digital dan mengembangkan keterampilan yang diperlukan untuk mengelola dan memanfaatkan data (Dwivedi et al., 2023).

Agrafiotis et al. (2018) mengidentifikasi berbagai jenis kerugian yang diakibatkan oleh serangan siber, termasuk kerugian fisik atau digital, kerugian ekonomi, kerugian psikologis, kerugian reputasi, dan kerugian sosial dan masyarakat. Cremer et al. (2022) menekankan perlunya data yang lebih baik untuk memahami dan mengelola risiko siber.

Untuk mengatasi ancaman keamanan siber, lembaga keuangan harus mengadopsi strategi mitigasi risiko yang komprehensif. Beberapa teknologi dan strategi kunci meliputi: Kerangka Kerja Keamanan yang Komprehensif: Penerapan kerangka kerja keamanan yang komprehensif, seperti NIST Cybersecurity Framework, dapat membantu lembaga keuangan mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari serangan siber (Stouffer et al., 2015). Investasi dalam Teknologi Keamanan Siber Canggih: Lembaga keuangan harus berinvestasi dalam teknologi keamanan siber canggih, seperti sistem deteksi intrusi, sistem pencegahan intrusi, *firewall*, dan solusi manajemen ancaman terpadu. Penggunaan AI dan *machine learning* (ML) untuk keamanan siber juga semakin penting (Gill et al., 2022; Butt et al., 2020; Capuano et al., 2022). Pengembangan Kesadaran Keamanan Siber: Pelatihan dan pendidikan karyawan tentang praktik keamanan siber yang baik sangat penting. Ini termasuk pelatihan tentang *phishing*, rekayasa sosial, dan praktik keamanan kata sandi. Manajemen Identitas dan Akses (IAM): Penerapan IAM yang kuat untuk mengontrol akses ke sistem dan data. Enkripsi: Penggunaan enkripsi untuk melindungi data sensitif, baik saat disimpan maupun saat transit. Respons Insiden: Pengembangan rencana respons insiden yang komprehensif untuk

menanggapi serangan siber dengan cepat dan efektif. Pemulihan Bencana: Penerapan rencana pemulihan bencana untuk memastikan kelangsungan bisnis jika terjadi serangan siber yang merusak. Audit dan Penilaian Keamanan: Melakukan audit dan penilaian keamanan secara teratur untuk mengidentifikasi kerentanan dan memastikan efektivitas kontrol keamanan. Kolaborasi: Kolaborasi antara lembaga keuangan, pemerintah, dan sektor swasta untuk berbagi informasi ancaman, praktik terbaik, dan respons terhadap insiden.

Jangirala et al. (2018) menyoroti pentingnya regulasi pemerintah dalam keamanan siber. Kiff et al. (2020) membahas pertimbangan keamanan siber terkait valuta digital bank sentral (CBDC). Tujuan dari penelitian ini adalah untuk menganalisis tantangan yang dihadapi oleh industri perbankan dalam menghadapi digitalisasi dan ancaman keamanan siber, serta mengidentifikasi strategi mitigasi risiko operasional yang efektif.

## Metode Penelitian

Penelitian ini menggunakan metode studi literatur komprehensif. Pendekatan ini melibatkan pengumpulan, analisis, dan sintesis informasi dari berbagai sumber, termasuk: **Publikasi Ilmiah:** Artikel jurnal yang diterbitkan dalam jurnal ilmiah terkemuka, seperti yang terindeks dalam database seperti Scopus dan Web of Science. **Laporan Industri:** Laporan dari perusahaan konsultan, lembaga riset, dan asosiasi industri yang relevan dengan digitalisasi perbankan dan keamanan siber.

Proses pengumpulan data melibatkan pencarian sistematis menggunakan kata kunci yang relevan, seperti "digitalisasi perbankan," "keamanan siber," "risiko operasional," "mitigasi risiko," "fintech," "ancaman siber," dan kombinasi dari kata kunci tersebut. Database elektronik seperti Scopus, Web of Science, Google Scholar, dan database lainnya digunakan untuk mengidentifikasi artikel dan publikasi yang relevan.

Analisis data dilakukan dengan mengidentifikasi tema utama, tren, dan kesenjangan dalam literatur. Informasi diekstraksi dari setiap sumber yang relevan, termasuk tujuan penelitian, metodologi, temuan utama, dan kesimpulan. Data dianalisis secara kualitatif untuk mengidentifikasi strategi mitigasi risiko yang efektif dan tantangan utama yang dihadapi oleh industri perbankan. Sintesis informasi dilakukan untuk menghasilkan pemahaman yang komprehensif tentang topik penelitian dan untuk mengembangkan kerangka kerja konseptual.

## Hasil dan Pembahasan

### Tantangan Utama Digitalisasi Perbankan

Digitalisasi perbankan menghadirkan sejumlah tantangan utama, terutama terkait dengan keamanan siber. Hasil studi literatur menunjukkan beberapa tantangan utama yang dihadapi oleh lembaga keuangan. Digitalisasi telah memperluas permukaan serangan, membuat lembaga keuangan lebih rentan terhadap serangan siber. Ketergantungan pada teknologi digital, termasuk aplikasi seluler, layanan *online*, dan sistem terhubung, menciptakan lebih banyak titik masuk bagi pelaku kejahatan siber. Ancaman siber terus berkembang dalam kompleksitas dan frekuensi. Pelaku kejahatan siber menggunakan teknik yang semakin canggih, seperti AI, *machine learning*, dan teknik rekayasa sosial, untuk melakukan serangan. Serangan *ransomware*, *phishing*, dan serangan DoS/DDoS semakin umum dan merugikan. (Choo, 2011; Khan et al.,

2019) Terdapat kekurangan keterampilan keamanan siber di industri perbankan. Lembaga keuangan kesulitan untuk merekrut dan mempertahankan profesional keamanan siber yang berkualitas. Hal ini membuat sulit untuk mengelola dan merespons ancaman siber secara efektif. Regulasi keamanan siber yang kompleks dan terus berubah menambah tantangan bagi lembaga keuangan. Lembaga keuangan harus mematuhi berbagai peraturan, termasuk GDPR, CCPA, dan standar industri seperti PCI DSS. (Jangirala et al., 2018) Lembaga keuangan semakin bergantung pada penyedia pihak ketiga, seperti penyedia layanan cloud, penyedia teknologi, dan mitra bisnis. Hal ini meningkatkan risiko keamanan siber, karena lembaga keuangan harus memastikan bahwa pihak ketiga juga memiliki praktik keamanan yang kuat.

**Strategi Mitigasi Risiko Operasional**

Studi literatur mengidentifikasi beberapa strategi mitigasi risiko operasional yang efektif untuk melindungi lembaga keuangan dari ancaman keamanan siber:

**Penerapan Kerangka Kerja Keamanan yang Komprehensif:**

Penerapan kerangka kerja keamanan yang komprehensif, seperti NIST Cybersecurity Framework, ISO 27001, atau COBIT, dapat membantu lembaga keuangan mengelola risiko keamanan siber secara sistematis. Kerangka kerja ini menyediakan panduan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari serangan siber (Stouffer et al., 2015). Kerangka kerja ini membantu dalam menyusun kebijakan dan prosedur keamanan, serta memastikan bahwa kontrol-kontrol keamanan diterapkan secara efektif.

**Investasi dalam Teknologi Keamanan Siber Canggih:**

Investasi dalam teknologi keamanan siber canggih sangat penting untuk melindungi aset dan data lembaga keuangan. Teknologi ini meliputi: Sistem memantau lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan yang dapat mengindikasikan serangan. IPS dapat secara otomatis memblokir serangan. *Firewall* NGFW menyediakan perlindungan yang lebih komprehensif, termasuk inspeksi paket mendalam, deteksi ancaman lanjutan, dan kontrol aplikasi. UTM menggabungkan berbagai fitur keamanan, seperti *firewall*, IDS/IPS, anti-virus, dan filter web, dalam satu perangkat. Solusi keamanan endpoint melindungi perangkat seperti laptop, *smartphone*, dan tablet dari ancaman siber. SIEM mengumpulkan dan menganalisis data keamanan dari berbagai sumber untuk mendeteksi dan merespons ancaman. SOAR mengotomatisasi tugas-tugas respons insiden untuk mempercepat dan meningkatkan efisiensi.

Penggunaan AI dan ML dalam keamanan siber semakin penting untuk mendeteksi dan merespons ancaman siber secara efektif (Gill et al., 2022; Butt et al., 2020; Capuano et al., 2022).

**Tabel 1**
**Ringkasan Strategi Mitigasi Risiko**

Tabel berikut merangkum strategi mitigasi risiko operasional yang dapat diterapkan oleh lembaga keuangan untuk mengatasi ancaman keamanan siber:

| Strategi | Deskripsi | Manfaat |
|---|---|---|
| Kerangka Kerja Keamanan yang Komprehensif | Penerapan kerangka kerja seperti NIST | Manajemen risiko sistematis, kepatuhan regulasi. |

| Strategi | Deskripsi | Manfaat |
|---|---|---|
| | Cybersecurity Framework. | |
| Investasi dalam Teknologi Keamanan Siber Canggih | IDS/IPS, *firewall* generasi berikutnya, SIEM, SOAR, dll. | Deteksi ancaman yang lebih baik, respons insiden yang cepat. |
| Pengembangan Kesadaran Keamanan Siber | Pelatihan dan pendidikan karyawan. | Pengurangan risiko kesalahan manusia, peningkatan kewaspadaan. |
| Manajemen Identitas dan Akses (IAM) | Autentikasi kuat, otorisasi berbasis peran. | Kontrol akses yang ketat, perlindungan data. |
| Enkripsi | Enkripsi data saat disimpan dan transit. | Perlindungan data sensitif. |
| Respons Insiden | Rencana respons insiden yang komprehensif. | Respons cepat dan efektif terhadap serangan. |
| Pemulihan Bencana | Backup data dan sistem, pemulihan dari lokasi alternatif. | Kelangsungan bisnis. |
| Audit dan Penilaian Keamanan | Penilaian kerentanan, pengujian penetrasi, audit kepatuhan. | Identifikasi kerentanan, peningkatan kontrol keamanan. |
| Kolaborasi | Berbagi informasi ancaman, kemitraan publik-swasta. | Peningkatan intelijen ancaman, respons kolektif. |

**Pembahasan**

Hasil penelitian ini mengkonfirmasi bahwa digitalisasi perbankan memberikan manfaat signifikan, tetapi juga meningkatkan risiko keamanan siber. Temuan ini sejalan dengan penelitian sebelumnya yang menunjukkan bahwa transformasi digital meningkatkan eksposur terhadap ancaman siber (Saeed et al., 2023). Digitalisasi telah memperluas permukaan serangan, menciptakan lebih banyak titik masuk bagi pelaku kejahatan siber. Ancaman siber juga terus berkembang dalam kompleksitas dan frekuensi, dengan serangan yang semakin canggih dan sulit dideteksi (Choo, 2011; Khan et al., 2019).

Penelitian ini mengidentifikasi beberapa strategi mitigasi risiko operasional yang efektif. Penerapan kerangka kerja keamanan yang komprehensif, seperti NIST Cybersecurity Framework, menyediakan kerangka kerja untuk mengelola risiko keamanan siber secara sistematis (Stouffer et al., 2015). Investasi dalam teknologi keamanan siber canggih, termasuk IDS/IPS, *firewall* generasi berikutnya, dan SIEM,

sangat penting untuk mendeteksi dan merespons ancaman siber secara efektif. Pengembangan kesadaran keamanan siber, manajemen identitas dan akses (IAM), enkripsi, respons insiden, pemulihan bencana, audit dan penilaian keamanan, dan kolaborasi juga merupakan komponen penting dari strategi mitigasi risiko yang komprehensif.

Temuan penelitian ini konsisten dengan penelitian sebelumnya yang menekankan pentingnya pendekatan holistik terhadap keamanan siber (Eling & Schnell, 2016). Lembaga keuangan harus mengadopsi pendekatan berlapis untuk keamanan, yang mencakup teknologi, proses, dan sumber daya manusia. Kolaborasi antara lembaga keuangan, pemerintah, dan sektor swasta sangat penting untuk berbagi informasi ancaman, praktik terbaik, dan respons terhadap insiden.

Implikasi dari penelitian ini adalah bahwa lembaga keuangan harus memprioritaskan keamanan siber sebagai bagian integral dari strategi bisnis mereka. Lembaga keuangan harus berinvestasi dalam teknologi keamanan siber canggih, mengembangkan kesadaran keamanan siber, dan menerapkan praktik keamanan yang baik. Mereka juga harus mematuhi regulasi keamanan siber yang relevan dan berkolaborasi dengan pemangku kepentingan lainnya untuk meningkatkan postur keamanan siber mereka.

Penelitian ini memiliki beberapa batasan. Studi literatur hanya mencakup publikasi yang tersedia secara publik. Selain itu, penelitian ini tidak mencakup analisis mendalam tentang efektivitas relatif dari berbagai strategi mitigasi risiko. Penelitian lebih lanjut diperlukan untuk mengatasi keterbatasan ini.

## Dampak Serangan Siber dan Kerugian Operasional

Serangan siber dapat menimbulkan dampak yang sangat merugikan bagi lembaga perbankan. Kerugian finansial akibat serangan siber dapat sangat besar, termasuk biaya pemulihan sistem, denda regulasi, biaya hukum, dan hilangnya pendapatan (Cremer et al., 2022). Selain itu, serangan siber dapat menyebabkan kerusakan reputasi yang signifikan, yang dapat mengakibatkan hilangnya kepercayaan pelanggan dan penurunan nilai saham. Gangguan operasional akibat serangan siber juga dapat mengganggu layanan perbankan, menyebabkan ketidaknyamanan bagi pelanggan, dan bahkan mengganggu stabilitas sistem keuangan secara keseluruhan (Eling & Schnell, 2016). Agrafiotis et al. (2018) mengidentifikasi berbagai jenis kerugian akibat serangan siber, yang mencakup kerugian finansial, kerugian reputasi, dan kerugian operasional.

## Strategi Mitigasi Risiko Operasional

Untuk menghadapi tantangan keamanan siber dalam era digitalisasi perbankan, lembaga keuangan perlu mengadopsi strategi mitigasi risiko operasional yang komprehensif. Strategi ini harus mencakup berbagai aspek, mulai dari peningkatan keamanan teknologi hingga peningkatan kesadaran dan pelatihan karyawan. Berikut adalah beberapa strategi mitigasi risiko yang efektif:

*1. Peningkatan Keamanan Teknologi*

Lembaga keuangan harus berinvestasi dalam teknologi keamanan yang canggih untuk melindungi sistem dan data mereka. Ini termasuk penggunaan firewall, sistem deteksi intrusi, sistem pencegahan intrusi, enkripsi data, dan otentikasi multi-faktor. Penting juga untuk secara teratur memperbarui perangkat lunak dan sistem untuk

menambal kerentanan keamanan. Stouffer et al. (2015) memberikan panduan tentang keamanan sistem kontrol industri (ICS), yang relevan dalam konteks perbankan karena banyak infrastruktur perbankan yang memanfaatkan sistem kontrol tersebut. Penerapan teknologi seperti 5G dan potensi implementasi 6G juga perlu dipertimbangkan, dengan tetap memperhatikan aspek keamanan yang menjadi perhatian utama (Khan et al., 2019; de Alwis et al., 2021).

*2. Manajemen Risiko yang Efektif*

Lembaga keuangan harus mengembangkan kerangka kerja manajemen risiko yang komprehensif untuk mengidentifikasi, menilai, dan mengelola risiko keamanan siber. Ini termasuk melakukan penilaian risiko secara berkala, mengembangkan kebijakan dan prosedur keamanan, dan menetapkan rencana tanggap darurat. Penting juga untuk memantau secara terus-menerus aktivitas jaringan dan sistem untuk mendeteksi dan merespons serangan siber secara tepat waktu. Cremer et al. (2022) menyoroti pentingnya ketersediaan data yang baik dalam manajemen risiko siber.

*3. Peningkatan Kesadaran dan Pelatihan Karyawan*

Karyawan adalah garis pertahanan pertama terhadap serangan siber. Oleh karena itu, lembaga keuangan harus memberikan pelatihan keamanan siber yang komprehensif kepada semua karyawan. Pelatihan harus mencakup topik-topik seperti phishing, malware, rekayasa sosial, dan praktik keamanan terbaik. Selain itu, lembaga keuangan harus meningkatkan kesadaran karyawan tentang pentingnya keamanan siber melalui kampanye informasi dan simulasi serangan siber. Persiapan tempat kerja untuk transformasi digital, termasuk pelatihan karyawan, merupakan aspek penting untuk keberhasilan (Trenerry et al., 2021).

*4. Kerja Sama dan Berbagi Informasi*

Lembaga keuangan harus bekerja sama dengan lembaga keuangan lain, pemerintah, dan penyedia keamanan siber untuk berbagi informasi tentang ancaman dan serangan siber. Berbagi informasi dapat membantu lembaga keuangan untuk mengantisipasi dan merespons serangan siber secara lebih efektif. Selain itu, lembaga keuangan harus berpartisipasi dalam forum industri dan inisiatif berbagi informasi untuk meningkatkan postur keamanan siber secara keseluruhan. Keterlibatan dalam ekosistem yang lebih luas, termasuk dengan lembaga riset dan akademisi, juga dapat memberikan wawasan berharga (Dwivedi et al., 2023).

*5. Penggunaan Teknologi Blockchain*

Teknologi *blockchain* memiliki potensi untuk meningkatkan keamanan dalam industri perbankan. Blockchain dapat digunakan untuk mengamankan transaksi, mencegah penipuan, dan meningkatkan transparansi. Blockchain juga dapat digunakan untuk menciptakan sistem identifikasi digital yang aman. Namun, perlu diingat bahwa teknologi *blockchain* juga memiliki tantangan tersendiri, termasuk masalah skalabilitas dan kompleksitas (Andoni et al., 2018; Wang et al., 2018). Osmani et al. (2020) menganalisis biaya, manfaat, risiko, dan peluang dari penerapan *blockchain* dalam perbankan.

*6. Pemanfaatan Kecerdasan Buatan (AI)*

Kecerdasan buatan (AI) dapat memainkan peran penting dalam meningkatkan keamanan siber. AI dapat digunakan untuk mendeteksi dan merespons serangan siber secara otomatis, menganalisis data keamanan untuk mengidentifikasi ancaman, dan meningkatkan efisiensi operasional keamanan. Namun, perlu diingat bahwa AI juga dapat digunakan oleh penyerang siber, sehingga lembaga keuangan harus mengambil

langkah-langkah untuk melindungi sistem AI mereka. Penggunaan AI dalam keamanan siber juga memerlukan pertimbangan etika dan transparansi (Capuano et al., 2022; Gill et al., 2022). Saniuk et al. (2022) membahas pergeseran transformasi industri menuju Industry 5.0 dengan mempertimbangkan aspek sosial dan ekonomi, yang juga relevan dalam konteks AI.

*7. Kepatuhan terhadap Regulasi*

Lembaga keuangan harus mematuhi semua peraturan dan standar keamanan siber yang relevan. Kepatuhan terhadap regulasi dapat membantu lembaga keuangan untuk mengurangi risiko keamanan siber dan melindungi data pelanggan. Pemerintah memainkan peran penting dalam menetapkan regulasi keamanan siber (Jangirala et al., 2018; OECD, 2019). Pemahaman yang komprehensif tentang regulasi dan standar industri sangat penting untuk memastikan kepatuhan.

*8. Asuransi Siber*

Asuransi siber dapat membantu lembaga keuangan untuk mengurangi dampak finansial dari serangan siber. Asuransi siber dapat memberikan perlindungan terhadap kerugian finansial akibat serangan siber, termasuk biaya pemulihan sistem, denda regulasi, dan biaya hukum (Eling & Schnell, 2016). Namun, penting untuk memilih polis asuransi siber yang tepat dan memahami ketentuan dan pengecualian dalam polis tersebut. Cremer et al. (2022) membahas kebutuhan akan sumber informasi yang lebih baik dan standarisasi dalam konteks asuransi siber.

**Tantangan dalam Implementasi Strategi Mitigasi Risiko**

Meskipun strategi mitigasi risiko operasional sangat penting, implementasinya tidak selalu mudah. Beberapa tantangan utama dalam implementasi strategi mitigasi risiko meliputi:

*1. Kompleksitas Ancaman Siber*

Ancaman siber terus berkembang dalam kompleksitas dan frekuensi. Penyerang siber terus mengembangkan teknik serangan baru yang lebih canggih dan sulit dideteksi. Lembaga keuangan harus terus beradaptasi dengan lanskap ancaman yang terus berubah untuk tetap efektif dalam melindungi diri mereka sendiri. Choo (2011) membahas lanskap ancaman siber dan arah penelitian di masa depan.

*2. Keterbatasan Sumber Daya*

Implementasi strategi mitigasi risiko yang efektif membutuhkan sumber daya yang signifikan, termasuk anggaran, personel, dan teknologi. Lembaga keuangan mungkin menghadapi keterbatasan sumber daya yang dapat menghambat kemampuan mereka untuk berinvestasi dalam teknologi keamanan yang canggih, merekrut dan mempertahankan ahli keamanan siber, dan memberikan pelatihan keamanan siber yang komprehensif. Keterbatasan sumber daya dapat menjadi hambatan signifikan, terutama bagi lembaga keuangan yang lebih kecil.

*3. Kurangnya Keterampilan Keamanan Siber*

Terdapat kekurangan keterampilan keamanan siber di seluruh dunia. Lembaga keuangan mungkin kesulitan untuk merekrut dan mempertahankan ahli keamanan siber yang berkualifikasi. Kurangnya keterampilan keamanan siber dapat menghambat kemampuan lembaga keuangan untuk mengimplementasikan dan mengelola strategi mitigasi risiko yang efektif. Hal ini memerlukan investasi dalam pendidikan dan pelatihan untuk mengembangkan tenaga kerja keamanan siber yang terampil.

*4. Perubahan Budaya Organisasi*

Implementasi strategi mitigasi risiko yang efektif seringkali memerlukan perubahan budaya organisasi. Karyawan harus memahami pentingnya keamanan siber dan bersedia untuk mematuhi kebijakan dan prosedur keamanan. Lembaga keuangan harus menciptakan budaya keamanan siber yang kuat, di mana keamanan siber menjadi prioritas utama bagi semua karyawan. Perubahan budaya organisasi bisa menjadi proses yang sulit dan memakan waktu.

*5. Kepatuhan terhadap Regulasi yang Kompleks*

Lembaga keuangan harus mematuhi berbagai peraturan dan standar keamanan siber yang kompleks. Kepatuhan terhadap regulasi dapat memakan waktu dan mahal. Lembaga keuangan harus memiliki sumber daya dan keahlian yang diperlukan untuk mematuhi semua peraturan yang relevan. Jangirala et al. (2018) membahas regulasi pemerintah dalam keamanan siber, termasuk kerangka kerja, standar, dan rekomendasi.

**Peran Pemerintah dan Regulator**

Pemerintah dan regulator memiliki peran penting dalam mendukung upaya mitigasi risiko keamanan siber dalam industri perbankan. Peran mereka meliputi:

*1. Penetapan Regulasi dan Standar*

Pemerintah dan regulator harus menetapkan regulasi dan standar keamanan siber yang jelas dan komprehensif. Regulasi dan standar harus mencakup berbagai aspek keamanan siber, termasuk persyaratan keamanan teknologi, manajemen risiko, dan pelaporan insiden. Regulasi dan standar harus diperbarui secara berkala untuk mencerminkan lanskap ancaman yang terus berubah. Jangirala et al. (2018) memberikan tinjauan tentang regulasi pemerintah dalam keamanan siber.

*2. Pengawasan dan Penegakan Hukum*

Pemerintah dan regulator harus melakukan pengawasan dan penegakan hukum untuk memastikan bahwa lembaga keuangan mematuhi regulasi dan standar keamanan siber. Pengawasan dan penegakan hukum harus dilakukan secara efektif dan konsisten. Penegakan hukum yang kuat dapat membantu mencegah serangan siber dan melindungi data pelanggan. Cremer et al. (2022) menyoroti kebutuhan akan pelaporan wajib dan kesadaran publik mengenai risiko siber.

*3. Berbagi Informasi dan Kerja Sama*

Pemerintah dan regulator harus memfasilitasi berbagi informasi dan kerja sama antara lembaga keuangan, pemerintah, dan penyedia keamanan siber. Berbagi informasi dapat membantu lembaga keuangan untuk mengantisipasi dan merespons serangan siber secara lebih efektif. Pemerintah dan regulator dapat memainkan peran penting dalam memfasilitasi berbagi informasi melalui pembentukan forum industri, inisiatif berbagi informasi, dan pusat informasi keamanan siber. Kerjasama internasional juga sangat penting dalam menghadapi ancaman siber lintas batas.

*4. Dukungan untuk Pendidikan dan Pelatihan*

Pemerintah dan regulator harus mendukung pendidikan dan pelatihan di bidang keamanan siber. Dukungan dapat mencakup pendanaan untuk program pendidikan dan pelatihan, pengembangan kurikulum, dan beasiswa untuk siswa yang tertarik dalam karir keamanan siber. Mendukung pengembangan tenaga kerja keamanan siber yang terampil sangat penting untuk memastikan bahwa lembaga keuangan memiliki keahlian yang diperlukan untuk melindungi diri mereka sendiri dari

ancaman siber. Dukungan ini juga dapat mencakup program kesadaran publik untuk meningkatkan pemahaman tentang keamanan siber di kalangan masyarakat umum.

*5. Penelitian dan Pengembangan*

Pemerintah dan regulator harus mendukung penelitian dan pengembangan di bidang keamanan siber. Dukungan dapat mencakup pendanaan untuk proyek penelitian, pengembangan teknologi keamanan baru, dan pengembangan praktik keamanan terbaik. Mendorong inovasi dalam teknologi keamanan siber sangat penting untuk memastikan bahwa lembaga keuangan memiliki alat yang diperlukan untuk menghadapi ancaman siber yang terus berkembang. Keterlibatan dalam penelitian dan pengembangan dapat membantu mengantisipasi ancaman di masa depan dan mengembangkan solusi yang efektif.

## Tantangan di Masa Depan dan Arah Penelitian

Digitalisasi perbankan akan terus berkembang di masa depan, dengan munculnya teknologi baru seperti kecerdasan buatan (AI), *blockchain*, dan komputasi kuantum. Perkembangan teknologi ini akan menimbulkan tantangan baru bagi keamanan siber yang memerlukan strategi mitigasi risiko yang lebih canggih dan adaptif. Beberapa tantangan di masa depan dan arah penelitian meliputi:

*1. Keamanan AI*

AI akan memainkan peran yang semakin penting dalam industri perbankan, termasuk dalam deteksi penipuan, analisis risiko, dan layanan pelanggan. Namun, AI juga dapat digunakan oleh penyerang siber untuk mengembangkan serangan yang lebih canggih dan sulit dideteksi. Penelitian di masa depan harus fokus pada pengembangan teknik keamanan AI untuk melindungi sistem AI dari serangan. Ini termasuk pengembangan algoritma yang lebih aman, teknik deteksi anomali, dan mekanisme pertahanan yang tangguh. Gill et al. (2022) membahas tren yang muncul dan arah masa depan dalam AI untuk komputasi generasi berikutnya.

*2. Keamanan Blockchain*

*Blockchain* memiliki potensi untuk meningkatkan keamanan dalam industri perbankan, tetapi juga memiliki kerentanannya sendiri. Penelitian di masa depan harus fokus pada pengembangan teknik keamanan yang lebih baik untuk melindungi sistem *blockchain* dari serangan. Ini termasuk pengembangan protokol konsensus yang lebih aman, teknik enkripsi yang lebih kuat, dan mekanisme deteksi dan respons serangan. Singh et al. (2021) membahas serangan keamanan, tantangan, dan solusi untuk jaringan IoT terdistribusi di masa depan menggunakan *blockchain*. Jaoude & Saadé (2019) memberikan tinjauan tentang aplikasi *blockchain* di berbagai domain.

*3. Keamanan Komputasi Kuantum*

Komputasi kuantum memiliki potensi untuk memecahkan algoritma enkripsi yang saat ini digunakan oleh lembaga keuangan. Penelitian di masa depan harus fokus pada pengembangan teknik enkripsi yang tahan terhadap serangan komputasi kuantum. Ini termasuk pengembangan algoritma kriptografi pasca-kuantum dan teknik untuk melindungi data sensitif dari serangan komputasi kuantum. Keamanan komputasi kuantum akan menjadi semakin penting seiring dengan perkembangan teknologi komputasi kuantum. Pemahaman tentang dampak komputasi kuantum pada keamanan siber sangat penting untuk menjaga keamanan sistem keuangan di masa depan.

*4. Keamanan IoT*

Internet of Things (IoT) akan semakin terintegrasi dengan industri perbankan, dengan perangkat IoT yang digunakan untuk berbagai aplikasi, seperti pembayaran, otentikasi, dan pemantauan keamanan. Namun, perangkat IoT seringkali memiliki kerentanan keamanan. Penelitian di masa depan harus fokus pada pengembangan teknik keamanan yang lebih baik untuk melindungi perangkat IoT dan data yang mereka hasilkan. Ini termasuk pengembangan protokol komunikasi yang lebih aman, teknik otentikasi yang lebih kuat, dan mekanisme deteksi dan respons serangan. Allioui & Mourdi (2023) mengeksplorasi potensi IoT untuk pertumbuhan dan stabilitas keuangan yang lebih baik.

*5. Keamanan dalam 5G dan 6G*

Jaringan 5G dan 6G akan menyediakan konektivitas yang lebih cepat dan andal untuk industri perbankan. Namun, jaringan ini juga akan menimbulkan tantangan keamanan baru, termasuk risiko serangan pada infrastruktur jaringan, kerentanan privasi, dan risiko serangan pada perangkat yang terhubung. Penelitian di masa depan harus fokus pada pengembangan teknik keamanan yang lebih baik untuk melindungi jaringan 5G dan 6G dari serangan. Ini termasuk pengembangan protokol keamanan yang lebih kuat, teknik enkripsi yang lebih canggih, dan mekanisme deteksi dan respons serangan. Khan et al. (2019) membahas survei tentang keamanan dan privasi teknologi 5G, sementara de Alwis et al. (2021) membahas survei tentang tren, aplikasi, persyaratan, teknologi, dan penelitian di masa depan untuk 6G.

*6. Privasi Data*

Digitalisasi perbankan menghasilkan sejumlah besar data pelanggan. Melindungi privasi data pelanggan sangat penting untuk menjaga kepercayaan pelanggan dan mematuhi peraturan privasi. Penelitian di masa depan harus fokus pada pengembangan teknik privasi data yang lebih baik, termasuk teknik enkripsi, teknik anonimisasi, dan teknik privasi diferensial. Quach et al. (2022) membahas ketegangan dalam privasi dan data yang disebabkan oleh teknologi digital.

*7. Explainable AI (XAI) dalam Keamanan Siber*

Penerapan AI dalam keamanan siber semakin luas, tetapi kompleksitas algoritma AI seringkali menyulitkan untuk memahami bagaimana keputusan dibuat. Penelitian masa depan harus berfokus pada pengembangan *Explainable AI* (XAI) dalam keamanan siber. XAI bertujuan untuk membuat keputusan AI lebih transparan dan mudah dipahami, yang memungkinkan analis keamanan untuk lebih memahami dan mempercayai hasil AI, serta mengidentifikasi potensi bias atau kesalahan. Capuano et al. (2022) memberikan survei tentang XAI dalam keamanan siber.

*8. Keamanan Siber dan Ketahanan Bisnis*

Perusahaan perlu meningkatkan fokus pada ketahanan bisnis dalam menghadapi ancaman siber. Ini melibatkan kemampuan untuk pulih dari serangan siber dengan cepat dan efektif, serta untuk terus beroperasi bahkan dalam situasi serangan. Penelitian masa depan harus berfokus pada pengembangan strategi dan teknologi untuk meningkatkan ketahanan bisnis dalam menghadapi ancaman siber. Saeed et al. (2023) membahas transformasi digital dan tantangan keamanan siber untuk ketahanan bisnis.

## Kesimpulan

Digitalisasi perbankan menawarkan banyak manfaat, tetapi juga menimbulkan tantangan signifikan terkait keamanan siber. Untuk melindungi diri dari ancaman siber yang terus berkembang, lembaga keuangan harus mengadopsi pendekatan proaktif dan holistik terhadap keamanan siber. Ini termasuk investasi dalam teknologi keamanan yang canggih, manajemen risiko yang efektif, peningkatan kesadaran dan pelatihan karyawan, kerja sama dan berbagi informasi, penggunaan teknologi *blockchain* dan AI, kepatuhan terhadap regulasi, dan asuransi siber. Pemerintah dan regulator memainkan peran penting dalam mendukung upaya mitigasi risiko keamanan siber melalui penetapan regulasi dan standar, pengawasan dan penegakan hukum, berbagi informasi dan kerja sama, dukungan untuk pendidikan dan pelatihan, serta penelitian dan pengembangan. Lembaga keuangan yang mengadopsi strategi mitigasi risiko yang komprehensif akan lebih mampu melindungi aset dan data mereka, menjaga kepercayaan pelanggan, dan memastikan stabilitas sistem keuangan. Menghadapi tantangan di masa depan memerlukan penelitian dan pengembangan berkelanjutan untuk mengatasi ancaman yang muncul, seperti keamanan AI, keamanan *blockchain*, dan keamanan komputasi kuantum. Dengan menerapkan strategi yang tepat dan terus beradaptasi dengan lanskap ancaman yang berubah, industri perbankan dapat memanfaatkan manfaat digitalisasi sambil meminimalkan risiko keamanan siber.

## Referensi


Abou Jaoude, J., & Saadé, R. G. (2019). Blockchain Applications – Usage in Different Domains. *IEEE Access, 7*, 108077–108094. https://doi.org/10.1109/access.2019.2902501

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. M. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Ahmad, N., Ullah, Z., Arshad, M. Z., Kamran, H. W., Scholz, M., & Han, H. (2021). Relationship between corporate social responsibility at the micro-level and environmental performance: The mediating role of employee pro-environmental behavior and the moderating role of gender. *Sustainable Production and Consumption, 28*, 1036–1046. https://doi.org/10.1016/j.spc.2021.02.034

Al-Emran, M., Koohang, A., Nord, J. H., Ooi, K.-B., Aw, E. C.-X., Baabdullah, A. M., Buhalis, D., Cham, T.-H., Dennis, C., Dutot, V., Dwivedi, Y. K., Hughes, L., Mogaji, E., Pandey, N., Phau, I., Raman, R., Sharma, A., Σιγάλα, M., Ueno, A., & Wong, L.-W. (2023). Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation. *Journal of Computer Information Systems, 63*(2), 1–24. https://doi.org/10.1080/08874417.2023.2165197

Allen, F., Gu, X., & Jagtiani, J. (2021). A Survey of Fintech Research and Policy Discussion. *Review of Corporate Finance, 3*(1), 1–74. https://doi.org/10.1561/114.00000007

Allioui, H., & Mourdi, Y. (2023). Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. *Sensors, 23*(19), 8015. https://doi.org/10.3390/s23198015

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2018). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics, 9*(9), 1379. https://doi.org/10.3390/electronics9091379

Candi, E., Terrinoni, A., Rufini, A., Chikh, A., Lena, A. M., Suzuki, Y., Sayan, B. S., Knight, R. A., & Melino, G. (2006). p63 is upstream of IKKα in epidermal development. *Journal of Cell Science, 119*(1), 115–123. https://doi.org/10.1242/jcs.03265

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable Artificial Intelligence in CyberSecurity: A Survey. *IEEE Access, 10*, 103580–103605. https://doi.org/10.1109/access.2022.3204171

hen, X. H., You, X., & Chang, V. (2021). FinTech and commercial banks' performance in China: A leap forward or survival of the fittest? *Technological Forecasting and Social Change, 173*, 121167. https://doi.org/10.1016/j.techfore.2021.120645

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(7), 429–440. https://doi.org/10.1016/j.cose.2011.08.004

Cremer, F., Sheehan, B., Fortmann, M., Negahdari Kia, A., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance Issues and Practice, 47*(3), 563–596. https://doi.org/10.1057/s41288-022-00266-6

de Alwis, C., Kalla, A., Pham, Q.-V., Kumar, P., Dev, K., Hwang, W.-J., & Liyanage, M. (2021). Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. *IEEE Open Journal of the Communications Society, 2*, 1153–1176. https://doi.org/10.1109/ojcoms.2021.3071496

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. A., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management, 75*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 465–487. https://doi.org/10.1108/jrf-09-2016-0122

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access, 7*, 174707–174731. https://doi.org/10.1109/access.2019.2895302

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., … Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. *Internet of Things, 19*, 100514. https://doi.org/10.1016/j.iot.2022.100514

Jangirala, S., Das, A. K., & Kumar, N. (2018). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 85*, 164–179. https://doi.org/10.1016/j.future.2018.09.063

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys & Tutorials, 21*(3), 2038–2062. https://doi.org/10.1109/comst.2019.2933899

Kiff, J., Alwazir, J., Davidovic, S., Farias, A., Khan, A., Khiaonarong, T., Malaika, M., Monroe, H., Sugimoto, N., Tourpe, H., & Zhou, P. (2020). A Survey of Research on Retail Central Bank Digital Currency. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3652492

Kickbusch, I., Piselli, D., Agrawal, A., Balicer, R. D., Banner, O., Adelhardt, M., Capobianco, E., Fabian, C., Gill, A. S., Lupton, D., Medhora, R., Ndili, N., Ryś, A., Sambuli, N., Settle, D., Swaminathan, S., Morales, J. V., Wolpert, M., Wyckoff, A., … Wong, B. L. H. (2021). The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world. *The Lancet, 398*(10314), 1705–1766. https://doi.org/10.1016/s0140-6736(21)01824-9

Koohang, A., Nord, J. H., Ooi, K.-B., Tan, G. W.-H., Al-Emran, M., Aw, E. C.-X., Baabdullah, A. M., Buhalis, D., Cham, T.-H., Dennis, C., Dutot, V., Dwivedi, Y. K., Hughes, L., Mogaji, E., Pandey, N., Phau, I., Raman, R., Sharma, A., Σιγάλα, M., … Wong, L.-W. (2023). Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation. *Journal of Computer Information Systems, 63*(2), 1–24. https://doi.org/10.1080/08874417.2023.2165197

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7–46. https://doi.org/10.1162/isec_a_00189

MacNeil, M. A., Chapman, D. D., Heupel, M. R., Simpfendorfer, C. A., Heithaus, M. R., Meekan, M. G., Harvey, E. S., Goetze, J. S., Kiszka, J. J., Bond, M. E., Currey-Randall, L. M., Speed, C. W., Sherman, C. S., Rees, M. J., Udyawer, V., Flowers, K. I., Clementi, G. M., Valentin-Albanese, J., Gorham, T., … Prasetyo, A. P. (2020). Global status and conservation potential of reef sharks. *Nature, 583*(7816), 212–218. https://doi.org/10.1038/s41586-020-2519-y

OECD. (2019). *Artificial Intelligence in Society*. https://doi.org/10.1787/eedfee77-en

Osmani, M., El-Haddadeh, R., Hindi, N., Janssen, M., & Weerakkody, V. (2020). Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of Enterprise Information Management, 33*(6), 1099–1127. https://doi.org/10.1108/jeim-02-2020-0044

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(3), 463–487. https://doi.org/10.1007/s11747-022-00845-y

Rufini, A., Agostini, M., Grespi, F., Tomasini, R., Sayan, B. S., Niklison-Chirou, M. V., Conforti, F., Velletri, T., Mastino, A., Mak, T. W., Melino, G., & Knight, R. A. (2011). p73 in Cancer. *Genes & Cancer, 2*(11), 1080–1088. https://doi.org/10.1177/1947601911408890

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

Saniuk, S., Grabowska, S., & Straka, M. (2022). Identification of Social and Economic Expectations: Contextual Reasons for the Transformation Process of Industry 4.0 into the Industry 5.0 Concept. *Sustainability, 14*(3), 1391. https://doi.org/10.3390/su14031391

Singh, S., Hosen, A. S. M. S., & Yoon, B. (2021). Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access, 9*, 18085–18100. https://doi.org/10.1109/access.2021.3051602

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. D., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. https://doi.org/10.6028/nist.sp.800-82r2

Trakadas, P., Simoens, P., Gkonis, P. K., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., Skármeta, A., Trochoutsos, C., Calvo, D., Lobo, T. P., Chintamani, K., Fernández, I., Arnáiz, A., Parreira, J. X., Petrali, P., Leligou, H. C., Karkazis, P. (2020). An Artificial Intelligence-Based Collaboration Approach in Industrial IoT Manufacturing: Key Concepts, Architectural