Prosiding Seminar Nasional Ilmu Manajemen Kewirausahaan dan Bisnis
Volume. 2 Nomor. 2, Tahun 2025
e-ISSN : 3048-2488, Hal. 548-556
DOI: https://doi.org/10.61132/prosemnasimkb.v2i2.232
Tersedia: https://prosiding.arimbi.or.id/index.php/PROSEMNASIMKB

API Sebagai Inti Produk Digital dan Risiko Operasional di Lingkungan Perusahaan Modern

Reza Irsyadul Anam*
Institut Teknologi dan Bisnis Dewantara, Indonesia
*Penulis korespondensi: reza.irsyadul@gmail.com[1]

Abstract. *APIs (Application Programming Interfaces) have become a key component in the development of modern digital products and the transformation of cloud-based services. Its ability to provide structured access to data and enable cross-platform integration makes APIs at the core of the enterprise's digital architecture. However, the high level of API openness poses increasingly complex security challenges, including potential data exploitation, injection attacks, credential misuse, and exploitation of business logic loopholes. This article examines the strategic role of APIs in the digital ecosystem, analyzes the operational risks that arise from API exposure, and evaluates the effectiveness of basic defense mechanisms such as API Gateways and Web Application Firewalls (WAFs). The findings of the study show that while both solutions play an important role in controlling access, filtering, and mitigating attacks at the surface layer, they have not been able to provide comprehensive protection against modern API threats that are dynamic, distributed, and often exploit weaknesses at the application and business logic levels. Therefore, a more holistic, layered, and sustainable API security approach is needed, including anomalous behavior detection, API abuse protection, and real-time monitoring to maintain the integrity and reliability of digital services.*

Keywords: *API gates; Cybersecurity; Digital Products; Shadow Fire; Web Application Firewall*

Abstrak. API (Application Programming Interface) telah menjadi komponen kunci dalam pengembangan produk digital modern dan transformasi layanan berbasis cloud. Kemampuannya dalam menyediakan akses terstruktur terhadap data serta memungkinkan integrasi lintas platform menjadikan API sebagai inti dari arsitektur digital enterprise. Namun, tingginya tingkat keterbukaan API memunculkan tantangan keamanan yang semakin kompleks, termasuk potensi eksploitasi data, serangan injeksi, penyalahgunaan kredensial, dan pemanfaatan celah logika bisnis. Artikel ini mengkaji peran strategis API dalam ekosistem digital, menganalisis risiko operasional yang muncul akibat eksposur API, serta mengevaluasi efektivitas mekanisme pertahanan dasar seperti API Gateway dan Web Application Firewall (WAF). Temuan studi menunjukkan bahwa meskipun kedua solusi tersebut berperan penting dalam mengontrol akses, melakukan filtering, dan mengurangi serangan pada lapisan permukaan, keduanya belum mampu memberikan perlindungan komprehensif terhadap ancaman API modern yang bersifat dinamis, terdistribusi, dan sering memanfaatkan kelemahan pada level aplikasi maupun logika bisnis. Oleh karena itu, dibutuhkan pendekatan keamanan API yang lebih holistik, berlapis, serta berkelanjutan, mencakup deteksi perilaku anomali, proteksi terhadap penyalahgunaan API, serta pemantauan real-time untuk menjaga integritas dan keandalan layanan digital.

Kata Kunci: API Gateway; Keamanan Siber; Produk Digital; Shadow API; Web Application Firewall

1. PENDAHULUAN

Perusahaan digital saat ini mengandalkan API untuk menghubungkan aplikasi, layanan, dan data secara dinamis. API menjadi penghubung antar sistem internal dan eksternal, memungkinkan integrasi layanan pelanggan, transaksi, otomasi bisnis, dan pemanfaatan cloud computing. Namun, semakin tingginya ketergantungan pada API menjadikannya target empuk bagi pelaku ancaman siber.

Menurut penelitian industri, 78% organisasi telah mengalami insiden keamanan terkait API, dan 44% di antaranya terkena denda dari regulator karena kelalaian melindungi data pelanggan. Oleh karena itu, penguatan postur keamanan terhadap API menjadi prioritas

Naskah Masuk: 13 September 2025; Revisi: 30 September 2025; Diterima: 31 Oktober 2025;
Tersedia: 20 November 2025

strategis. Meskipun demikian, banyak perusahaan, terutama usaha kecil dan menengah, masih belum sepenuhnya memahami celah risiko keamanan jaringan komputer yang terkait dengan API, padahal insiden siber tidak hanya menyerang perusahaan besar (Haryadi et al., 2021). Kesadaran akan keamanan informasi, terutama dalam perlindungan data pribadi, masih perlu ditingkatkan di banyak perusahaan, karena kelalaian ini dapat merugikan reputasi dan nilai kompetitif mereka (Apriany & Wibowo, 2024).

Pengelolaan keamanan siber yang komprehensif, termasuk mitigasi risiko dari serangan siber, menjadi krusial untuk melindungi integritas sistem informasi, perangkat lunak, dan perangkat keras (Herdiana et al., 2021). Optimalisasi keamanan ini meliputi penerapan kebijakan Information Security Management System yang robust, di mana pemimpin organisasi memegang peranan krusial dalam memastikan kepatuhan dan edukasi karyawan terkait disiplin ISMS (Sidabutar, 2024).

Latar Belakang

Dalam konteks ini, peningkatan penetrasi jaringan global dan kemajuan mobile internet di Indonesia turut memperparah kerentanan keamanan informasi organisasi terhadap ancaman siber, menjadikan serangan siber sebagai tantangan utama bagi pemangku kebijakan (Islami, 2018). Sebagai contoh, insiden serangan siber WannaCry pada tahun 2017 menunjukkan dampak masif yang dapat ditimbulkan, mengganggu operasional perusahaan dan rumah sakit di lebih dari 150 negara, termasuk Indonesia (Islami, 2018). Isu ini menyoroti pentingnya strategi mitigasi yang efektif untuk meminimalisir risiko yang terkait dengan kejahatan siber, yang menggunakan teknologi informasi sebagai alat maupun targetnya (Chintia et al., 2019). Terlebih lagi, kejahatan siber, yang mencakup penipuan, pencurian kekayaan intelektual, dan pelanggaran privasi, semakin sering terjadi seiring dengan berkembangnya fungsi internet sebagai pusat perdagangan dan pemerintahan, menuntut peningkatan perlindungan data dan aset penting organisasi (Herdiana et al., 2021) (Idellie & Atok, 2023).

2. RUMUSAN MASALAH

Berangkat dari permasalahan tersebut, studi ini bertujuan untuk merumuskan rumusan masalah yang akan menjadi fokus analisis, yaitu bagaimana mengidentifikasi dan mengelola risiko operasional yang timbul dari penggunaan API dalam arsitektur produk digital, serta mengevaluasi efektivitas solusi keamanan siber yang ada dalam memitigasi risiko tersebut. Selain itu, penelitian ini juga akan menganalisis tantangan implementasi strategi keamanan siber nasional di Indonesia dan mengidentifikasi rekomendasi untuk peningkatan kapabilitas keamanan API di masa mendatang (Islami, 2018). Fokus penelitian ini juga mencakup analisis

mendalam terhadap evolusi ancaman siber dan dampaknya terhadap ekosistem API, serta mengidentifikasi praktik terbaik dalam tata kelola keamanan API.

3. HASIL DAN PEMBAHASAN

Tujuan Penelitian

Studi ini bertujuan untuk memberikan pemahaman komprehensif mengenai risiko operasional yang inheren pada penggunaan API dalam pengembangan produk digital modern dan mengevaluasi efektivitas solusi keamanan siber yang relevan, seperti API Gateway dan Web Application Firewall, dalam mengatasi ancaman tersebut (Ali, 2021). Penelitian ini juga bertujuan untuk mengidentifikasi celah dalam pendekatan keamanan siber saat ini dan merekomendasikan strategi yang lebih adaptif untuk melindungi API dari serangan yang semakin canggih, terutama dengan mempertimbangkan peningkatan jumlah pengguna teknologi informasi yang berpotensi menjadi target kejahatan siber (Chintia et al., 2019).

Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan kerangka kerja keamanan API yang lebih kuat dan adaptif, serta meningkatkan kesadaran akan pentingnya perlindungan infrastruktur API di lingkungan bisnis yang semakin terhubung.

API sebagai Inti Produk Digital

API mendukung berbagai fungsi penting, seperti:

Interkoneksi layanan mikro (*microservices*) dengan platform eksternal dan pihak ketiga Otomatisasi proses bisnis Integrasi. Arsitektur *microservices* adalah pendekatan rekayasa perangkat lunak yang memecah sistem besar menjadi kumpulan layanan kecil dan independen, masing-masing berfokus pada satu fungsi bisnis [Newman, 2015]. Setiap layanan ini dapat dikembangkan, diuji, dan dideploy secara terpisah, yang memungkinkan iterasi cepat dan skalabilitas tinggi. Komunikasi antar layanan dilakukan melalui protokol ringan berbasis API, menjadikan API sebagai *pintu masuk dan keluar* utama dari setiap microservice.

Paradigma ini semakin relevan di era digital, di mana sistem monolitik tidak lagi mampu menjawab kebutuhan bisnis yang dinamis. Penggunaan microservices memberikan euntungan dalam hal: Isolasi kesalahan (fault isolation). Fleksibilitas dalam pemilihan teknologi. Skalabilitas berdasarkan kebutuhan per layanan. Ketahanan (resilience) terhadap perubahan system. Integrasi dengan mitra bisnis (B2B). Layanan pelanggan berbasis aplikasi mobile dan web. Otomasi proses bisnis dan penggunaan AI/ML.

Integrasi dengan mitra bisnis (B2B)

Integrasi sistem dalam konteks *Business-to-Business (B2B)* kini bergeser dari pendekatan tradisional berbasis *point-to-point* menjadi pendekatan modern berbasis API terbuka dan microservices. Tujuannya adalah mendukung fleksibilitas, otomatisasi layanan, dan kolaborasi dinamis antar organisasi. Dengan adanya standar nasional seperti SNAP BI di sektor perbankan, integrasi B2B kini harus tidak hanya cepat dan efisien, tetapi juga memenuhi kepatuhan regulasi dan keamanan data.

Arsitektur Microservices Internal

a. Sistem inti dibangun dengan pendekatan *microservices*, yang menjadikan setiap fitur atau layanan sebagai modul independen.
b. Memungkinkan organisasi untuk mengekspos hanya layanan relevan kepada mitra tanpa membuka seluruh sistem.

API Gateway dan Open API Standards

a. Mengelola semua permintaan dari mitra eksternal melalui satu titik kontrol.
b. Menerapkan protokol standar (REST, JSON, OAuth2) untuk kompatibilitas dan keamanan.

Mitra Bisnis Eksternal (B2B Clients)

a. Pihak ketiga seperti fintech, asuransi, e-commerce, logistik, dll.
b. Mengakses layanan melalui API yang didokumentasikan dan dibatasi oleh kebijakan akses (*rate limiting*, *authorization scope*).

Orkestrasi dan Otomatisasi Proses Bisnis

a. Proses lintas organisasi seperti *order fulfillment*, *payment initiation*, *settlement*, dan *reconciliation* diotomatisasi melalui integrasi API.
b. BPM (Business Process Management) digunakan untuk menyatukan proses backend antar organisasi.

Manajemen Keamanan dan Kepatuhan API

a. Pengawasan lalu lintas API, autentikasi, logging, dan audit untuk memenuhi standar keamanan seperti ISO 27001, PCI-DSS, atau SNAP BI.
b. Termasuk deteksi *shadow APIs*, *misconfiguration*, dan pencegahan *data leakage*.

Risiko Operasional yang Terkait API

Risiko mencakup shadow API, kesalahan konfigurasi, kebocoran data, dan penyalahgunaan API. Risiko ini semakin diperparah dengan kompleksitas arsitektur microservices dan kebutuhan akan integrasi yang mulus dengan berbagai pihak eksternal (Pranata et al., 2018).

a. **Shadow API**: API yang tidak terdokumentasi atau tidak diketahui oleh tim keamanan. Hal ini menciptakan celah keamanan signifikan, memungkinkan akses tidak sah dan eksploitasi oleh aktor jahat (Siriwardena, 2014).
b. **Misconfigurations**: Pengaturan keamanan yang lemah atau keliru, seperti tidak adanya autentikasi atau validasi input. Kerentanan ini dapat membuka jalan bagi serangan injeksi, pengungkapan data sensitif, atau bahkan pengambilalihan sistem.
c. **Data Exposure**: Pengiriman data sensitif tanpa enkripsi atau pembatasan akses. Ancaman terhadap sistem informasi juga meliputi interupsi, intersepsi, dan modifikasi data, yang semuanya dapat menyebabkan kerusakan signifikan pada integritas dan ketersediaan informasi (Saputra et al., 2023).
d. **Rate Limiting Abuse**: Serangan brute force melalui permintaan API yang berlebihan. Penyalahgunaan ini dapat menyebabkan penolakan layanan atau akses tidak sah ke data melalui percobaan kredensial berulang (Bhuiyan et al., 2018).

Perlindungan Dasar: API Gateway dan Web Application Firewall (WAF)

Sebagian besar organisasi menggunakan dua komponen utama sebagai proteksi awal terhadap ancaman berbasis API dan web, yaitu API Gateway dan Web Application Firewall (Munsch & Munsch, 2021). Kedua komponen ini menyediakan lapisan pertahanan pertama yang krusial dalam mitigasi risiko operasional, meskipun dengan fokus dan kapabilitas yang berbeda.

API Gateway

API Gateway berfungsi sebagai pintu masuk terpusat untuk semua permintaan API. Fitur utamanya mencakup:

a. Autentikasi dan otorisasi (mis. OAuth2, API key)
b. Rate limiting dan throttling
c. Routing dan logging trafik API
d. Pengaturan versi API

Kelebihan:

✓ Mendukung pengelolaan API secara terstruktur
✓ Melindungi dari serangan sederhana seperti DDoS ringan
✓ Memudahkan audit dan monitoring

Kekurangan:

× Hanya mengamankan API yang terdaftar (tidak mendeteksi shadow API)
× Tidak melakukan analisa keamanan secara mendalam terhadap payload

Web Application Firewall (WAF)

WAF dirancang untuk menyaring dan memantau lalu lintas HTTP/HTTPS ke aplikasi web. Fitur WAF antara lain:

a. Perlindungan terhadap serangan umum (mis. SQL Injection, XSS)
b. Analisa permintaan dan respons HTTP
c. Integrasi dengan sistem deteksi ancaman

Kelebihan:

✓ Memberikan lapisan pertahanan tambahan terhadap ancaman aplikasi web
✓ Umum digunakan dan mudah diimplementasikan

Kekurangan:

× Tidak khusus untuk API (kurang sensitif terhadap pola-pola API)
× Terbatas dalam menganalisis struktur data seperti JSON/XML

Keterbatasan dan Tantangan

Ancaman seperti validasi logika bisnis dan inspeksi payload membutuhkan solusi keamanan API modern, Pendekatan ini diperlukan untuk mengatasi kompleksitas serangan yang semakin canggih, terutama yang mengeksploitasi kerentanan pada tingkat fungsional dan data (Paryati, 2015), yang sering luput dari deteksi oleh API Gateway dan WAF tradisional (Umar et al., 2019).

a. Inspeksi payload dalam format non-standar

Payload non-standar, seperti format data yang disesuaikan atau terenkripsi, dapat menyulitkan WAF dan API Gateway untuk melakukan inspeksi mendalam dan deteksi anomali secara efektif (Bermbach & Wittern, 2016).

Hal ini sering terjadi pada API yang menggunakan GraphQL, di mana fleksibilitasnya dalam pengambilan data dapat mempersulit validasi skema dan keamanan secara otomatis (Muntahanah et al., 2024).

b. Validasi logika bisnis API

Serangan yang mengeksploitasi cacat dalam alur logika aplikasi tidak dapat dideteksi oleh mekanisme keamanan statis, melainkan memerlukan analisis dinamis terhadap interaksi API (Matondang et al., 2018).

Sebagai contoh, penyalahgunaan fungsionalitas API untuk mengakses data yang tidak seharusnya, meskipun permintaan tersebut secara sintaksis valid, merupakan celah yang sering dimanfaatkan oleh penyerang.

c. Eksploitasi parameter tersembunyi

Parameter tersembunyi dalam API, yang tidak terekspos secara eksplisit dalam dokumentasi tetapi dapat dimanipulasi oleh penyerang, menjadi vektor serangan yang sulit dideteksi oleh solusi keamanan konvensional (Mayasari et al., 2020).

Dalam hal ini memerlukan solusi keamanan API yang khusus seperti:

a. API behavior analytics

Pendekatan berbasis analisis perilaku trafik API untuk mengidentifikasi deviasi dari pola normal, sering kali didukung oleh unsupervised learning. Ini memungkinkan deteksi anomali yang menunjukkan serangan siber yang kompleks, seperti penyalahgunaan kredensial atau eksfiltrasi data, yang mungkin tidak terdeteksi oleh aturan keamanan berbasis tanda tangan tradisional.

b. Runtime protection

Solusi ini secara aktif memantau eksekusi kode API untuk mencegah eksploitasi kerentanan zero-day dan serangan yang memanfaatkan logika bisnis yang cacat, dengan menerapkan kebijakan keamanan secara adaptif.

Mekanisme keamanan yang bekerja langsung di lapisan eksekusi aplikasi atau API—yakni saat aplikasi sedang berjalan—untuk mendeteksi dan mencegah serangan secara real-time

c. Continuous API testing

Pengujian API secara berkelanjutan ini mencakup fuzz testing, penemuan kerentanan, dan validasi fungsional untuk memastikan bahwa setiap perubahan pada API tidak memperkenalkan celah keamanan baru atau regresi fungsional. Pendekatan ini sangat penting untuk mempertahankan postur keamanan API yang proaktif dan responsif terhadap lanskap ancaman yang terus berkembang.

d. Discovery tools untuk shadow API

Alat ini secara proaktif mengidentifikasi API yang tidak terdokumentasi dan tidak terkelola, memastikan visibilitas penuh terhadap semua titik akhir API yang berpotensi menjadi target serangan (Darojat et al., 2022). Tujuan dari identifikasi ini adalah untuk memperkirakan nilai risiko pada setiap peralatan, yang kemudian dapat digunakan untuk merancang rencana inspeksi yang sesuai, mengelola risiko kegagalan, dan meningkatkan prioritas berdasarkan nilai risiko yang terukur (Rozie, 2022).

4. SIMPULAN DAN REKOMENDASI

API telah menjadi tulang punggung produk dan layanan digital, namun sekaligus menjadi vektor ancaman baru yang terus berkembang. Penggunaan API Gateway dan WAF merupakan fondasi penting dalam membangun postur keamanan API. Namun, perusahaan perlu melengkapi pendekatan ini dengan strategi keamanan API yang lebih komprehensif, termasuk pemantauan runtime, deteksi anomali, dan pengelolaan siklus hidup API.

Rekomendasi:

Implementasi API Gateway sebagai kontrol akses dan manajemen trafik. Integrasi WAF untuk mitigasi serangan umum. Investasi dalam platform keamanan API yang proaktif. Edukasi tim pengembang dan keamanan tentang risiko API. Inventarisasi dan pengujian berkala terhadap semua API (termasuk shadow API

REFERENCES

Ali, I. (2021). Examining cyber security implementation through TLS/SSL on academic institutional repository in Indonesia. *Berkala Ilmu Perpustakaan dan Informasi, 17*(2), 238. https://doi.org/10.22146/bip.v17i2.2082

Apriany, A., & Wibowo, A. (2024). Analysis of the implementation of ISO 27001: 2022 and KAMI Index in enhancing the information security management system in consulting firms. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 18*(4). https://doi.org/10.22146/ijccs.100385

Bermbach, D., & Wittern, E. (2016). Benchmarking Web API quality. In *Lecture notes in computer science* (p. 188). Springer. https://doi.org/10.1007/978-3-319-38791-8_11

Bhuiyan, T., Begum, A., Rahman, S., & Hadid, I. (2018). API vulnerabilities: Current status and dependencies. *International Journal of Engineering & Technology, 7*(2.3), 9. https://doi.org/10.14419/ijet.v7i2.3.9957

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, M. (2019). Kasus kejahatan siber yang paling banyak terjadi di Indonesia dan penanganannya. *Journal of Information Engineering and Educational Technology, 2*(2), 65–69. https://doi.org/10.26740/jieet.v2n2.p65-69

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability assessment website e-government dengan NIST SP 800-115 dan OWASP menggunakan Web Vulnerability Scanner. *Jurnal Sistem Informasi Bisnis, 12*(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44

Haryadi, E., Yuliandari, D., Abdussomad, A., Wijayanti, D., Amelia, M., & Syafrianto, S. (2021). Maintaining the continuity of the company's operation using the NIST framework for SME. *Jurnal Teknik Komputer, 7*(1), 74–82. https://doi.org/10.31294/jtk.v7i1.9486

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi ancaman risiko keamanan siber di masa pandemi COVID-19. *Jurnal ICT Information Communication & Technology, 20*(1), 42–50. https://doi.org/10.36054/jict-ikmi.v20i1.305

Idellie, P. L., & Atok, R. M. (2023). Pemodelan distribusi kerugian siber dengan pendekatan copula dan perhitungan premi asuransi siber. *Jurnal Sains dan Seni ITS, 12*(1). https://doi.org/10.12962/j23373520.v12i1.97479

Islami, M. J. (2018). Tantangan dalam implementasi strategi keamanan siber nasional Indonesia ditinjau dari penilaian Global Cybersecurity Index. *Masyarakat Telematika dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi, 8*(2), 137–150. https://doi.org/10.17933/mti.v8i2.108

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis manajemen risiko keamanan data sistem informasi (Studi kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2*(1), 282–290. https://doi.org/10.29207/resti.v2i1.96

Mayasari, R., Ridha, A. A., Juardi, D., & Baihaqi, K. A. (2020). Analisis vulnerability pada website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability. *Systematics, 2*(1), 33–39. https://doi.org/10.35706/sys.v2i1.3450

Munsch, A., & Munsch, P. (2021). The future of API (Application Programming Interface) security: The adoption of APIs for digital communications and the implications for cyber security vulnerabilities. *Journal of International Technology and Information Management, 29*(3), 24–39. https://doi.org/10.58729/1941-6679.1454

Muntahanah, M., Darmi, Y., & Pinandita, K. (2024). Implementasi perbandingan metode GraphQL dan REST API pada teknologi Node.js. *INTECOMS Journal of Information Technology and Computer Science, 7*(1), 25–35. https://doi.org/10.31539/intecoms.v7i1.8656

Paryati, P. (2015). Keamanan sistem informasi. *Seminar Nasional Informatika (SEMNASIF), 1*(4). http://jurnal.upnyk.ac.id/index.php/semnasif/article/download/743/621

Pranata, B. A., Hijriani, A., & Junaidi, A. (2018). Perancangan Application Programming Interface (API) berbasis web menggunakan gaya arsitektur Representational State Transfer (REST) untuk pengembangan sistem informasi administrasi pasien klinik perawatan kulit. *Jurnal Komputasi, 6*(1), 33–44. https://doi.org/10.23960/komputasi.v6i1.1554

Rozie, A. F. (2022). Analisis keselamatan dan kelayakan penggunaan CNG buffer storage tank berbasis metode residual life assessment. *AME (Aplikasi Mekanika dan Energi) Jurnal Ilmiah Teknik Mesin, 8*(1), 48–57. https://doi.org/10.32832/ame.v8i1.6194

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). Ancaman keamanan pada sistem informasi manajemen perusahaan. *Jurnal Pendidikan Siber Nusantara, 1*(2), 58–68. https://doi.org/10.38035/jpsn.v1i2.48

Sidabutar, J. (2024). Analisa sistem manajemen keamanan informasi (SMKI) organisasi menggunakan Indeks KAMI. *Journal of Information and Technology, 4*(2), 50–60. https://doi.org/10.32938/jitu.v4i2.7747

Siriwardena, P. (2014). *Advanced API security*. Apress. https://doi.org/10.1007/978-1-4302-6817-8

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis, 9*(1), 47–54. https://doi.org/10.21456/vol9iss1pp47-54