JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 04, No. 01, Tahun 2025, Hal.2486-2496, ISSN: 3031-9498 (Online)

Analisis Keamanan *Cloud Computing* dalam Meningkatkan Daya Saing UMKM: *Systematic Literatur Review*

Erik Agustian[1], Muhamad Farhan[2], Yusuf Fadhil Marzuqi[3]
[1,2,3]Universitas Pamulang, Indonesia
E-mail: erikagustian3805@gmail.com[1], farhan20020309@gmail.com[2], yusuffm6233@gmail.com[3]

Article Info

Article history:

Received December 09, 2025
Revised December 14, 2025
Accepted December 19, 2025

Keywords:

Cloud Computing Security, Competitiveness of MSMEs, Cyber Security Digital Transformation, Systematic Literature Review

ABSTRACT

The digital transformation of micro, small, and medium enterprises (MSMEs) depends on cloud computing. However, the main obstacle to its adoption continues to be cybersecurity threats. The purpose of this study is to evaluate the role of cloud security in improving the competitiveness of MSMEs. The SLR method was conducted by identifying, selecting, and synthesizing scientific articles from various national and international databases using predetermined inclusion criteria and the PRISMA framework. The results of the study show that MSMEs can strengthen their competitiveness by increasing trust, operational efficiency, and innovation capabilities with good cloud security. However, a lack of cybersecurity awareness, limited resources, and infrastructure constraints are issues that MSMEs still face. This study found that MSME development can be strategically supported through the implementation of effective cloud security. This requires a holistic approach that combines technological elements, human resources, and supporting policies.

Article Info

Article history:

Received December 09, 2025
Revised December 14, 2025
Accepted December 19, 2025

Kata Kunci:

Keamanan Cloud Computing, Daya Saing UMKM, Keamanan Cyber Transformasi Digital, Systematic Literatur Review

ABSTRACT

Transformasi digital bisnis mikro, kecil, dan menengah (UMKM) bergantung pada cloud computing. Namun, hambatan utama untuk adopsinya terus menjadi ancaman keamanan siber. Tujuan dari penelitian ini adalah untuk mengevaluasi peran keamanan cloud dalam meningkatkan daya saing UMKM. Metode SLR dilakukan dengan mengidentifikasi, menyeleksi, dan mensintesis artikel ilmiah dari berbagai database nasional dan internasional menggunakan kriteria inklusi yang telah ditetapkan dan kerangka PRISMA. Hasil penelitian menunjukkan bahwa UMKM dapat memperkuat daya saing mereka dengan meningkatkan kepercayaan, efisiensi operasional, dan kemampuan inovasi dengan keamanan cloud yang baik. Namun, kurangnya kesadaran keamanan siber, keterbatasan sumber daya, dan kendala infrastruktur adalah masalah yang masih dihadapi oleh UMKM. Studi ini menemukan bahwa pengembangan UMKM dapat dibantu secara strategis melalui penerapan keamanan cloud yang efektif. Ini memerlukan pendekatan holistik yang menggabungkan elemen teknologi, sumber daya manusia, dan kebijakan pendukung.

JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 04, No. 01, Tahun 2025, Hal.2486-2496, ISSN: 3031-9498 (Online)

Corresponding Author:

Erik Agustian
Universitas Pamulang
Email: erikagustian3805@gmail.com

PENDAHULUAN

Di era ekonomi yang semakin terhubung ini, cloud computing telah menjadi pilar penting untuk transformasi digital usaha mikro, kecil, dan menengah (UMKM). Teknologi ini tidak memerlukan investasi infrastruktur TI yang signifikan, tetapi memungkinkan UMKM untuk mengoptimalkan operasional, meningkatkan produktivitas, dan memperluas jangkauan pasar dengan memberikan akses ke sumber daya komputasi yang fleksibel, skalabel, dan hemat biaya (Arisandy et al., 2024). Dalam pasar global, penggunaan cloud computing dianggap sebagai strategi penting untuk meningkatkan daya saing, inovasi, dan ketahanan UMKM.

Namun, adopsi teknologi cloud tidak terlepas dari masalah sulit, terutama yang berkaitan dengan keamanan siber. Karena risiko seperti kebocoran data, serangan ransomware, akses ilegal, dan masalah konfigurasi sistem, banyak perusahaan kecil dan menengah (UMKM) tidak dapat memanfaatkan sepenuhnya potensi cloud computing (Alkadrie & Fitroh, 2024). Adoption platform digital lain seperti TikTok Seller menghadapi masalah serupa. UMKM di Parung Panjang awalnya menghadapi kesulitan karena tidak memahami teknologi dan keterampilan digital (Fauzi et al., 2025). Padahal keamanan data yang dikelola dengan baik dapat meningkatkan persaingan dan menumbuhkan kepercayaan pelanggan, kekhawatiran tentang keamanan data sering kali membuat pengambilan keputusan menjadi ragu.

Hanya 30,8% UMKM yang mengakui telah melakukan pencegahan yang memadai terhadap serangan siber, meskipun 46,2% dari mereka pernah mengalaminya (Suartana et al., 2024). Keterbatasan ini menunjukkan bahwa intervensi edukatif yang terorganisir diperlukan. Sebuah program sosialisasi keamanan digital yang menggunakan simulasi ancaman dan pelatihan interaktif telah terbukti dapat meningkatkan pemahaman peserta secara signifikan. Lebih dari 85 persen peserta meningkatkan skor mereka (Eriana et al., 2025). Dengan meningkatkan pengetahuan tentang keamanan digital, UMKM dapat mempersiapkan diri untuk menghadapi ancaman siber. Mereka juga dapat memasukkan praktik keamanan cloud ke dalam strategi bisnis mereka, yang pada akhirnya akan mendukung peningkatan daya saing dan ketahanan di era digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis peran keamanan cloud computing dalam meningkatkan daya saing UMKM. Dengan mengkaji temuan penelitian terbaru, studi ini mencoba menjawab pertanyaan tentang bagaimana praktik keamanan cloud dapat dioptimalkan untuk mendukung pertumbuhan, ketahanan, dan kompetitivitas UMKM di tengah transformasi digital yang semakin cepat.

METODE PENELITIAN

Untuk menganalisis hubungan antara keamanan cloud computing dan peningkatan daya saing usaha mikro, kecil, dan menengah (UMKM), penelitian ini menggunakan metodologi Systematic Literature Review (SLR). Sesuai dengan pedoman PRISMA, metode SLR mencakup fase identifikasi literatur, penyaringan, evaluasi kelayakan, ekstraksi data, analisis tematik, dan perumusan kesimpulan sistematis. Metodologi ini dipilih karena kemampuan untuk menemukan pola temuan penelitian, menemukan kesenjangan dalam penelitian, dan menyusun sintesis pengetahuan yang koheren melalui tahapan analitis dan evaluasi yang sistematis (Alkadrie & Fitroh, 2024).

Menyusun Pertanyaan Penelitian

Sebagai langkah awal dalam merumuskan pertanyaan penelitian yang tepat, peneliti menerapkan kerangka PICOC (Population, Intervention, Comparison, Outcome, Context) untuk mendefinisikan cakupan dan fokus kajian secara jelas.

Komponen PICOC	Deskripsi dalam Konteks Penelitian Ini
Population (Populasi)	Usaha Mikro, Kecil, dan Menengah (UMKM) atau MSMEs, sebagai subjek utama yang mengadopsi teknologi cloud.
Intervention (Intervensi)	Implementasi dan manajemen keamanan cloud computing (seperti enkripsi, kontrol akses, pemantauan, kebijakan keamanan) pada UMKM.
Comparison (Perbandingan)	Kondisi UMKM sebelum dan setelah menerapkan keamanan cloud, atau perbandingan antara UMKM yang menerapkan keamanan cloud dengan yang tidak.
Outcome (Hasil)	Peningkatan daya saing UMKM, yang diukur melalui parameter: kepercayaan pelanggan, efisiensi operasional, inovasi digital, ketahanan bisnis, dan kepatuhan regulasi.
Context (Konteks)	Lingkungan bisnis digital di Indonesia pascapandemi, dengan fokus pada transformasi digital, ancaman siber, dan kerangka regulasi keamanan data.

Tabel 2 menunjukkan struktur desain pertanyaan penelitian yang digunakan peneliti untuk membuat pertanyaan penelitian. Pertanyaan-pertanyaan ini dibuat berdasarkan kebutuhan topik yang dipilih. Pertanyaan penelitian berikut adalah.

ID	Research Question	Tujuan
RQ1	Bagaimana tingkat kesadaran dan pemahaman UMKM terhadap keamanan cloud computing?	Mengukur kesiapan dan literasi keamanan digital UMKM.
RQ2	Ancaman keamanan siber apa yang paling sering dihadapi UMKM dalam penggunaan cloud?	Memetakan pola ancaman dan kerentanan utama.
RQ3	Bagaimana implementasi keamanan cloud dapat meningkatkan daya saing UMKM?	Menganalisis dampak keamanan terhadap kepercayaan, efisiensi, dan inovasi bisnis.
RQ4	Apa saja hambatan dan strategi efektif dalam mengadopsi keamanan cloud bagi UMKM?	Mengidentifikasi solusi dan rekomendasi berbasis konteks lokal.

Strategi Pencarian Literatur

Dalam penelitian ini, panduan PRISMA digunakan sebagai dasar untuk proses pencarian literatur. Untuk melakukan pencarian, pengguna menggunakan basis data nasional dan internasional seperti Google Scholar, GARUDA Kemendikbud, SINTA (Index Sains dan Teknologi), dan platform OJS dari beberapa universitas (seperti UNS, UAJY, UPI, UNISNU, dan UNUD). Keamanan cloud, keamanan cloud, kesadaran cybersecurity, UMKM, persaingan, transformasi digital, dan kombinasi operator Boolean adalah beberapa kata kunci yang digunakan. Publikasi dibatasi dari tahun 2021 hingga 2025 untuk tetap relevan dengan perkembangan terbaru. Identifikasi, penyaringan, penilaian kelayakan, dan inklusi adalah langkah-langkah yang digunakan dalam protokol SLR untuk menyelesaikan proses seleksi artikel.

Kriteria Inklusi dan Eksklusi

Kriteria Inklusi:

1. Artikel yang membahas isu keamanan (security), risiko, tantangan, atau strategi dalam adopsi dan implementasi cloud computing pada Usaha Mikro, Kecil, dan Menengah (UMKM).
2. Diterbitkan dalam rentang tahun 2020–2025.
3. Artikel berupa hasil penelitian empiris, kajian literatur sistematis (SLR), studi kasus, atau penelitian kualitatif/kuantitatif yang dipublikasikan dalam jurnal ilmiah bereputasi atau prosiding konferensi yang tereview.
4. Tersedia dalam format teks lengkap (full-text) dan dapat diakses secara terbuka (open access) atau melalui langganan institusi peneliti.
5. Ditulis dalam bahasa Indonesia atau Inggris.

Kriteria Eksklusi:

1. Artikel yang tidak secara spesifik membahas UMKM atau hanya membahas cloud computing tanpa dimensi keamanan.
2. Artikel yang diterbitkan sebelum tahun 2020.
3. Artikel non-ilmiah seperti blog, majalah populer, laporan media, atau opini tanpa dasar metodologi penelitian.
4. Artikel yang hanya tersedia dalam bentuk abstrak, berbayar tanpa akses, atau tidak lengkap.
5. Artikel yang ditulis dalam bahasa selain Indonesia atau Inggris tanpa tersedia terjemahan resmi.

HASIL DAN PEMBAHASAN

A. Bagaimana tingkat kesadaran dan pemahaman UMKM terhadap keamanan cloud computing?

Berdasarkan kajian literatur yang relevan dengan topik penelitian ini menunjukkan bahwa pemahaman dan kesadaran Usaha Mikro, Kecil, dan Menengah (UMKM) tentang masalah keamanan cloud computing sangat rendah. Ini juga merupakan titik penting dalam transformasi digital mereka. Seseorang tidak benar-benar tahu apa yang mereka lakukan; sebaliknya, mereka

berada dalam keadaan "kesadaran yang cemas tetapi tidak berdaya" di mana kekhawatiran akan ancaman siber ada, tetapi tidak sebanding dengan pengetahuan dan kemampuan mereka untuk mengelola risiko tersebut dengan baik.

Selama periode 2020–2022, Badan Siber dan Sandi Negara (BSSN) menerapkan struktur PAMAN KAMI, yang merupakan bukti paling jelas dari rendahnya pemahaman ini. Secara konsisten, hasil survei 844 UMKM di berbagai wilayah Indonesia menunjukkan hasil yang didominasi oleh kategori "BURUK" dan "KURANG" (Ajhari et al., 2023). Hasil empiris ini menunjukkan bahwa fondasi kesadaran dan praktik keamanan di tingkat UMKM masih sangat lemah. Hasil ini bukan sekadar persepsi, tetapi pengukuran nyata tentang kematangan keamanan informasi. Data yang menunjukkan bahwa hampir setengah (46.2%) dari pelaku UMKM yang disurvei mengaku pernah mengalami serangan siber membuat situasi ini lebih buruk (Suartana et al., 2024). Ironisnya, sebagian besar responden menyatakan bahwa mereka belum atau tidak yakin telah melakukan upaya pencegahan yang memadai sebagai akibat dari pengalaman buruk ini. Hal ini menunjukkan perbedaan yang signifikan antara kemampuan untuk bertindak proaktif dan kesadaran akan adanya ancaman.

Karena pemahaman yang terbatas, kekhawatiran keamanan data ini kemudian menjadi penghalang utama dalam keputusan untuk menggunakan cloud computing. Selama sepuluh tahun (2011-2020), tinjauan literatur sistematis telah menunjukkan bahwa UMKM menghadapi masalah besar terkait keamanan data dan ketidakpercayaan terhadap penyedia layanan (Permana & Hadi, 2025). Studi kualitatif di Indonesia memperkuat persepsi ini, karena pelaku UMKM, khususnya di sektor jasa, menyatakan bahwa mereka khawatir tentang keamanan data dan kemungkinan kebocoran informasi. Selain itu, studi empiris yang menggunakan metode PLS-SEM menunjukkan bahwa kekhawatiran keamanan berdampak negatif secara statistik terhadap keinginan untuk menggunakan cloud computing (Hoxha & Aliko, 2023). Dengan kata lain, kekhawatiran tentang pelanggaran data dan akses ilegal, yang berasal dari pemahaman yang tidak lengkap, menghalangi UMKM untuk memanfaatkan potensi skalabilitas dan efisiensi teknologi cloud.

Dua masalah utama dapat dikaitkan dengan penyebab rendahnya kesadaran dan tingginya kecemasan ini. Pertama, pelaku UMKM masih kekurangan literasi digital, terutama di luar pusat kota (Pattiasina, 2025). Mereka tidak dapat memahami konsep keamanan siber yang lebih kompleks, seperti enkripsi, autentikasi multi-faktor, dan kebijakan tanggung jawab berbagi cloud, jika mereka tidak memahami cara teknologi digital bekerja. Kedua, tidak semua orang memiliki akses ke instruksi dan pelatihan yang relevan tentang keamanan siber. (Suartana et al., 2024) secara tegas menyimpulkan bahwa kurangnya pengetahuan dan pemahaman tentang keamanan cyber bagi pelaku UMKM adalah penyebab serangan siber yang sering terjadi (Suartana et al., 2024). Terbukti bahwa peserta lebih memahami acara sosialisasi dan pelatihan tentang keamanan cyber , menunjukkan bahwa pemberdayaan melalui pengetahuan adalah solusi untuk masalah ini.

Oleh karena itu, dapat disimpulkan bahwa UMKM masih memahami keamanan cloud computing secara tidak lengkap dan penuh kecemasan. Mungkin mereka telah mendengar tentang ancaman phishing atau kebocoran data, tetapi tidak banyak orang yang tahu bagaimana memitigasinya atau menilai kredibilitas penyedia layanan cloud. Paradoks yang ditimbulkan oleh situasi ini terjadi ketika takut akan risiko menghalangi perusahaan untuk menggunakan

teknologi yang, jika digunakan dengan aman, dapat meningkatkan daya saing dan ketahanan mereka. Akibatnya, upaya strategis untuk mendorong UMKM untuk menggunakan cloud computing harus diiringi dengan gerakan nasional untuk meningkatkan literasi digital dan keamanan siber yang inklusif, mudah dipahami, dan dapat diterapkan secara langsung dalam operasional UMKM tertentu. Selain itu, upaya ini tidak boleh hanya berfokus pada penyediaan akses atau insentif finansial. Tanpa landasan pemahaman yang solid, kekhawatiran akan tetap menjadi penghalang, dan kemungkinan transformasi digital melalui cloud computing tidak akan pernah terwujud sepenuhnya.

B. Ancaman keamanan siber apa yang paling sering dihadapi UMKM dalam penggunaan cloud ?

Berdasarkan kajian literatur yang relevan dengan topik penelitian, lanskap ancaman keamanan siber bagi Usaha Mikro, Kecil, dan Menengah (UMKM) saat menggunakan teknologi cloud sangat kompleks dan mencakup banyak aspek. Ancaman-ancaman ini tidak hanya bersifat teknis, tetapi juga sangat dipengaruhi oleh sumber daya yang terbatas dan kerentanan manusiawi, yang merupakan ciri khas banyak usaha kecil dan menengah (UMKM). Dari berbagai ancaman yang diidentifikasi, ancaman yang paling sering dihadapi adalah kebocoran data, yang disebabkan oleh akses tidak sah, dan ancaman internal. Serangan malware, phishing, dan ransomware adalah ancaman yang paling sering dihadapi.

Salah satu ancaman terbesar adalah kebocoran data. Kebocoran data menjadi salah satu ancaman paling signifikan dalam sistem cloud computing... sering kali disebabkan oleh ancaman dari dalam organisasi (ancaman insider), Berdasarkan penelitian (Majid Tanjung et al., 2025) Ancaman ini dapat berasal dari karyawan atau pihak berwenang yang secara sengaja atau tidak sengaja menyalahgunakan data sensitif. Data kuantitatif dari penelitian mendukung temuan kualitatif (Nagahawatta et al., 2021). Menurut data survei yang dilakukan terhadap 289 UMKM di Australia, akses tidak sah merupakan ancaman, dengan usaha mikro (21,9%), kecil (19,8%), dan menengah (20,6%) yang melaporkannya. Lebih menarik lagi, ancaman dari pihak dalam yang berniat jahat (malicious insiders) secara signifikan lebih tinggi dialami oleh usaha menengah (13%) dibandingkan dengan usaha mikro (5,1%) dan kecil (7,2%). Ini menunjukkan bahwa, seiring dengan

Selain kebocoran data, rekayasa sosial dan ancaman berbasis perangkat lunak berbahaya adalah masalah utama. berdasarkan penelitian (Nagahawatta et al., 2021) menunjukkan bahwa ancaman phishing, malware, dan ransomware cukup sering terjadi, terutama pada usaha mikro (13.8%). berdasarkan penelitian (Harianja, Simanullang, 2023) juga menyebutkan bahwa ini adalah jenis ancaman cybercrime yang umum menyerang bisnis digital. Serangan phishing yang memanfaatkan kelalaian manusia sangat efektif untuk menyerang UMKM yang seringkali tidak memiliki program pelatihan kesadaran keamanan yang cukup untuk karyawannya.

Di luar ancaman-ancaman utama tersebut, kesalahan konfigurasi platform cloud adalah kelemahan yang sering terjadi. Berdasarkan penellitian (Nagahawatta et al., 2021), usaha kecil menunjukkan keprihatinan yang lebih besar tentang masalah ini. Hal ini menunjukkan bahwa UMKM seringkali tidak memiliki tenaga ahli IT yang cukup untuk menyiapkan dan mengelola lingkungan cloud dengan konfigurasi keamanan yang ketat. Kesalahan dalam mengatur hak

akses atau pengaturan default yang tidak diubah dapat dengan mudah meninggalkan celah bagi penyerang.

Penelitian lain menjelaskan konteks mengapa ancaman-ancaman ini begitu sering menghantui UMKM. Studi kasus Kenya (Neyole et al., 2024) dan studi komparatif Australia (Nagahawatta et al., 2021) sama-sama menunjukkan keterbatasan sumber daya sebagai masalah utama. Karena keterbatasan anggaran, tidak ada investasi yang diperlukan untuk alat keamanan khusus, solusi pemantauan real-time seperti SIEM (Security Information and Event Management), atau asuransi siber. Selain itu, kekurangan tenaga kerja ahli menyebabkan kurangnya staf IT atau ahli keamanan siber. Seperti yang ditunjukkan dalam Tabel (Neyole et al., 2024), persentase UMKM dengan profesional keamanan cloud terlatih jauh lebih tinggi pada usaha menengah (13,2 persen) dan kecil (12,6 persen). Ini berbeda dengan usaha mikro (7,5 persen). Akibatnya, pemilik usaha atau karyawan dengan pengetahuan teknis yang terbatas seringkali dibebankan tanggung jawab keamanan.

Secara keseluruhan, diskusi literatur menunjukkan bahwa ancaman keamanan siber bagi UMKM di cloud adalah nyata, beragam, dan diperparah oleh keterbatasan sumber daya yang alami. Serangan berbasis malware/phishing dan kebocoran data adalah ancaman yang paling sering dilaporkan. Di sisi lain, kerentanan seperti misconfigurasi terus menjadi masalah teknis. Oleh karena itu, pendekatan keamanan untuk UMKM tidak dapat sepenuhnya meniru pendekatan yang digunakan perusahaan besar. Ia harus praktis, murah, dan berfokus pada mengurangi risiko tertinggi terutama yang melibatkan faktor manusia melalui pelatihan kesadaran keamanan (kesedaran keamanan), penerapan autentikasi multi-faktor (autentikasi multi-faktor), dan pengelolaan hak akses yang ketat. Itu harus didukung oleh solusi teknis dasar seperti enkripsi data dan pembaruan sistem rutin.

C. Bagaimana implementasi keamanan cloud dapat meningkatkan daya saing UMKM?

Berdasarkan kajian literatur yang relevan dengan topik penelitian ini menunjukkan bahwa penerapan keamanan cloud computing telah meningkatkan daya saing usaha mikro, kecil, dan menengah (UMKM) selain menjadi kebutuhan teknis. Kepercayaan pelanggan dan reputasi bisnis bergantung pada keamanan cloud. (Pattiasina, 2025) menekankan bahwa masalah keamanan data sering menjadi penghalang utama adopsi cloud. Namun, UMKM dapat membedakan diri di pasar dan memberikan jaminan kepada pelanggan dengan menerapkan langkah-langkah keamanan yang terlihat dan terukur, seperti sistem autentikasi yang kuat untuk aplikasi akuntansi berbasis cloud (Novitasari et al., 2023). Ini sangat penting karena kehilangan kepercayaan pelanggan adalah efek langsung dari kebocoran data (Rozi et al., 2024).

Selain itu, keamanan yang kuat secara langsung berkontribusi pada stabilitas dan kelangsungan operasi perusahaan. penelitian (Rahmawati & Nasution, 2024) menegaskan bahwa manfaat efisiensi operasional dari sistem berbasis cloud hanya dapat diperoleh jika sistem tersebut aman dan tersedia. Keamanan cloud melindungi UMKM dari gangguan operasional yang merugikan seperti serangan siber atau kehilangan data (Rozi et al., 2024), yang memungkinkan bisnis berjalan lancar dan fokus pada pertumbuhan.

Dari segi undang-undang, keamanan cloud yang memadai membuka pasar yang lebih luas. Berdasarkan penelitian (Darmawan, 2025), kerangka hukum perlindungan data memberikan kepastian untuk transformasi digital UMKM. Dengan menggunakan solusi cloud

yang memenuhi standar keamanan industri tertentu, seperti enkripsi dan kontrol akses ketat untuk industri keuangan atau kesehatan (Rozi et al., 2024), UMKM tidak hanya mematuhi hukum tetapi juga membangun kredibilitas untuk bekerja sama dengan perusahaan yang lebih besar atau bergabung dengan platform digital tertentu.

Rasa aman mendorong adopsi teknologi digital yang lebih maju. Setelah kekhawatiran keamanan diatasi, UMKM mulai tertarik untuk memanfaatkan solusi cloud yang meningkatkan efisiensi, seperti sistem manajemen dan pemasaran digital (Rahayu & Veri, 2025) atau ERP berbasis SaaS (Darmawan, 2025). Pada akhirnya, digitalisasi ini menjadi penyetara, memungkinkan UMKM bersaing dengan perusahaan besar karena efisiensi, fleksibilitas, dan akses ke teknologi canggih (Pattiasina, 2025).

Oleh karena itu, keamanan cloud berkembang dari menjadi biaya tambahan menjadi investasi yang dipertimbangkan secara strategis. Ia mematuhi peraturan, menjaga reputasi aset, dan memastikan operasi berlanjut. Yang paling penting, ia memungkinkan transformasi digital yang mendalam. Keunggulan kompetitif yang berkelanjutan diperlukan oleh UMKM untuk memiliki keamanan cloud yang andal dalam lingkungan bisnis modern.

D. Apa saja hambatan dan strategi efektif dalam mengadopsi keamanan cloud bagi UMKM?

Sebagai hasil dari analisis yang dilakukan terhadap enam jurnal referensi, adopsi keamanan cloud untuk perusahaan kecil dan menengah (UMKM) merupakan proses yang diwarnai oleh banyak tantangan yang berbeda, tetapi dapat diatasi melalui strategi yang terarah dan realistis. Faktor internal dan eksternal organisasi adalah sumber masalah utama. Secara internal, hambatan paling nyata adalah keterbatasan keuangan, di mana biaya awal untuk pelatihan, migrasi, dan infrastruktur dianggap sangat mahal (Abudaqqa, 2025). Karena kurangnya literasi digital dan kesadaran akan pentingnya keamanan siber, UMKM enggan beralih dari sistem konvensional, meskipun mereka lebih efektif (Oriza & Maulidar, 2024). Secara eksternal, ketidakpastian hukum meningkat karena struktur peraturan yang tidak jelas, terutama dalam hal jurisdiksi data dan tanggung jawab atas pelanggaran (Abudaqqa, 2025).

Keamanan data kini menjadi masalah psikologis yang paling penting. Bisnis kecil dan menengah (UMKM) yang menyimpan informasi pribadi seperti data pelanggan dan transaksi keuangan sangat khawatir akan ancaman kebocoran data, ransomware, dan akses ilegal dari pihak ketiga (Korespondensi, 2025). Ketakutan ini sering diperburuk oleh kekurangan sumber daya manusia teknis di dalam UMKM; sebagian besar dari mereka tidak memiliki karyawan IT khusus yang mampu mengelola, mengonfigurasi, dan memantau lingkungan cloud secara mandiri(Arroji et al., 2025). Karena ketergantungan tinggi pada penyedia layanan dan kurangnya pemahaman tentang mekanisme keamanan yang tersedia, ada banyak kerentanan dan ketidakpercayaan.

Strategi yang efektif harus dimulai dengan membangun fondasi pengetahuan untuk mengatasi tantangan tersebut. Langkah pertama yang sangat penting adalah meningkatkan literasi digital melalui program pelatihan khusus untuk pemilik dan karyawan UMKM. Pendidikan ini harus mencakup pengetahuan dasar tentang praktik keamanan dasar dan manajemen risiko siber (Oriza & Maulidar, 2024). Pada tingkat teknis, peningkatan ketahanan dengan biaya yang relatif terjangkau dapat dicapai dengan menerapkan prosedur keamanan

dasar seperti enkripsi data, autentikasi multi-faktor, dan prosedur backup rutin (Korespondensi, 2025). Selain itu, keputusan strategis penting adalah memilih model layanan yang tepat, dengan Software-as-a-Service (SaaS) sebagai pintu masuk yang ideal karena kemudahan dan prediktabilitas biayanya (Ahmad et al., 2025).

Untuk mempercepat adopsi yang aman, kerja sama multipihak sangat penting. Melalui regulasi yang jelas, insentif fiskal, dan program pendampingan, pemerintah memainkan peran penting dalam membangun ekosistem pendukung. Sementara itu, penyedia layanan cloud harus merancang solusi yang benar-benar sesuai dengan kebutuhan dan kemampuan UMKM, serta membangun transparansi dan kepercayaan melalui dukungan teknis yang mudah diakses (Abudaqqa, 2025; Oriza & Maulidar, 2024). Di Indonesia, Kerangka Kerja Keamanan Siber Nasional (KKSN) dari BSSN dapat dijadikan panduan bertahap bagi UMKM untuk membangun kapabilitas keamanan, dimulai dari identifikasi aset kritis hingga penyusunan rencana pemulihan (Arroji et al., 2025).

Internalisasi budaya keamanan siber dalam organisasi harus menjadi fokus strategi jangka panjang. Keamanan tidak boleh dianggap sebagai tugas teknis departemen tertentu; itu harus dilihat sebagai nilai penting dan tanggung jawab bersama yang terintegrasi dalam setiap proses bisnis. Komitmen dan dukungan aktif dari manajemen puncak sangat penting untuk penetapan kebijakan dan alokasi sumber daya (Ahmad et al., 2025). Pembangunan budaya ini, bersama dengan pandangan pengguna tentang keamanan cloud mobile dari (Ula et al., 2021), akan membentuk ketahanan organisasi yang berkelanjutan.

Secara keseluruhan, adopsi cloud computing yang aman bagi UMKM dapat dicapai, meskipun ada beberapa tantangan. Cloud computing dapat berubah dari sumber kekhawatiran menjadi pengungkit potensi yang kuat bagi UMKM untuk mencapai efisiensi, inovasi, dan daya saing yang lebih tinggi di era ekonomi digital. Ini dapat dicapai melalui pendekatan bertahap yang menggabungkan peningkatan kapasitas internal, pemanfaatan teknologi yang sesuai, dan sinergi dengan ekosistem eksternal.

KESIMPULAN

Berdasarkan hasil Systematic Literature Review yang telah dilakukan, Penelitian ini mengonfirmasi bahwa keamanan cloud computing merupakan komponen penting dalam meningkatkan daya saing Usaha Mikro, Kecil, dan Menengah (UMKM). Penemuan ini didasarkan pada analisis sistematis dari literatur yang relevan. Hanya 30,8% pelaku usaha yang mengakui telah mengambil tindakan pencegahan yang memadai, menunjukkan bahwa mayoritas UMKM masih menghadapi perbedaan antara kesadaran akan ancaman siber dan kemampuan teknis untuk mengelola risiko tersebut. Kebocoran data, serangan phishing, ransomware, dan kerentanan akibat miskonfigurasi sistem, yang diperparah oleh kekurangan dana dan sumber daya manusia berpengalaman.

Sebaliknya, praktik keamanan cloud yang tepat dapat meningkatkan kepercayaan pelanggan, memastikan keberlangsungan operasional, mematuhi peraturan, dan memberi UMKM akses ke teknologi digital yang lebih canggih. Oleh karena itu, keamanan cloud membantu transformasi digital dan bersaing. Strategi berlapis, yang mencakup edukasi berkelanjutan, penerapan kontrol keamanan dasar, pemilihan model layanan yang tepat, dan kerja sama dengan ekosistem pendukung seperti pemerintah dan penyedia layanan cloud, dapat

membantu mengatasi tantangan seperti literasi digital yang rendah, kekhawatiran akan kerahasiaan data, dan kerumitan regulasi.

Secara keseluruhan, penelitian ini menegaskan bahwa UMKM dapat bertahan dan berkembang dengan investasi dalam keamanan cloud sebagai langkah strategis. Rekomendasi untuk penelitian mendatang mencakup pengembangan kerangka keamanan cloud yang kontekstual untuk UMKM serta studi empiris untuk mengukur dampak langsung praktik keamanan terhadap kinerja usaha dan daya saing dalam jangka panjang.

DAFTAR PUSTAKA

Abudaqqa, F. (2025). Challenges in Cloud Computing Adoption for SMEs in the Middle East. *European Scientific Journal, ESJ*, *21*(3), 13. https://doi.org/10.19044/esj.2025.v21n3p13

Ahmad, C. S., Mahomed, A. S. B., & Hashim, H. (2025). Cloud Computing Adoption in SMEs: Exploring IaaS, PaaS and SaaS through a Bibliometric Study. *International Journal of Academic Research in Business and Social Sciences*, *15*(1), 1423–1446. https://doi.org/10.6007/ijarbss/v15-i1/24452

Ajhari, A. A., Manaon, M. A., & Dimas. (2023). Security Awareness Framework untuk Usaha Mikro, Kecil dan Menenengah di Indonesia. *Info Kripto*, *17*(3), 85–91. https://doi.org/10.56706/ik.v17i3.80

Alkadrie, S. A., & Fitroh. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, *4*(2), 1–15. https://doi.org/10.24002/konstelasi.v4i2.10277

Arisandy, A. Y., Permatasari, S. Della, Izaroh, S., Hidayat, R., & Ikaningtyas, M. (2024). Adopsi Cloud Computing Dalam Perencanaan Dan Pengembangan Bisnis Usaha Kecil Menengah (UKM). *Economics And Business Management Journal (EBMJ)*, *3*(1), 1–10. https://ejournal-rmg.org/index.php/EBMJ/article/view/192

Arroji, M. B., Rauf, A. A., Talia, L. D., Servanda, Y., & Insan, P. P. (2025). *Analisis Risiko Keamanan Siber pada Infrastruktur Digital UMKM di Balikpapan dan Strategi Mitigasi Berbasis Kerangka Kerja Keamanan Siber Nasional*. *8*(11), 1–9.

Darmawan, A. (2025). Penerapan Cloud Enterprise Resource Planning (Erp) Saas Untuk Usaha Kecil Menengah (Sme) Di Indonesia. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, *9*(1), 3018–3028. https://doi.org/10.31955/mea.v9i1.5548

Eriana, E. S., Zein, A., Wati, E. F., & Buminata, M. S. A. (2025). *SOSIALISASI KEAMANAN DIGITAL UNTUK MENGATASI PHISHING DAN APK BERBAHAYA*. 85–90. https://ejournal.stais-garut.ac.id/index.php/attamkiim

Fauzi, I., Wanto, D. O. E., & Iqbal, M. (2025). *Optimalisasi Strategi Digital Marketing Umkm Dengan Memanfaatkan Kecerdasan Bisnis Untuk Meningkatkan Penjualan Bagi Organisasi Masyarakat Pemuda*. *1*(2), 71–78.

Harianja, Simanullang, & R. (2023). Jurnal Ilmu Ekonomi dan Bisnis. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. http://repository.upm.ac.id/1199/

Hoxha, K., & Aliko, D. (2023). Cloud Computing Adoption in Albania: An Empirical Study. *CEUR Workshop Proceedings*, *3402*, 28–34.

Korespondensi, P. (2025). *STRATEGI KEAMANAN DALAM CLOUD COMPUTING ANALISIS ANCAMAN DAN SOLUSI MITIGASI*. *2*(1), 8–17.

Majid Tanjung, A., Lase, A., Zega, O., & Lafau, R. O. (2025). Keamanan Siber Dalam Sistem Informasi Berbasis Cloud: Tantangan Dan Solusi. *Jurnal Ilmu Ekonomi Dan Teknik*, *02*(01), 1–7.

Nagahawatta, R., Lokuge, S., Warren, M., & Salzman, S. (2021). Cybersecurity Issues and Practices in a Cloud Context: A Comparison Amongst Micro, Small and Medium Enterprises. *ACIS 2021 - Australasian Conference on Information Systems, Proceedings*, 1–11.

Neyole, J., Minado Okwiri, S., & Mapema, N. (2024). *Exploring the Impact of Cybersecurity Threats on Small and Medium Enterprises' Performance: A Case Study of Kajiado County, Kenya*. https://doi.org/10.20944/preprints202411.0237.v1

Novitasari, Agha, R. Z., Redyanti, G., Vidyasari, R., & Mahatmyo, A. (2023). *EFEKTIVITAS PEMANFAATAN CLOUD ACCOUNTING DALAM PENGELOLAAN KEUANGAN UMKM*. *22*(2), 209–216.

Oriza, R., & Maulidar. (2024). Adoption and Impact of Cloud Computing in Small and Medium Enterprises A Systematic Review. *Journal Informatic, Education and Management (JIEM)*, *6*(2), 8–15. https://doi.org/10.61992/jiem.v6i2.79

Pattiasina, T. (2025). Studi Kualitatif tentang Adopsi Cloud Computing pada UMKM di Indonesia. *Catha : Journal of Creative and Innovative Research*, *2*(1), 3046–8760.

Permana, N., & Hadi, S. P. (2025). Analisis Sistematis Adopsi Cloud Computing pada UMKM: Tren, Kerangka Teori, dan Faktor Pendorong dalam Satu Dekade (2011-2020). *Studia Ekonomika*, *23*(2), 16–32. https://www.jurnal-mnj.stiekasihbangsa.ac.id/index.php/StudiaEkonomika

Rahayu, W., & Veri, J. (2025). Penerapan Sistem Informasi Manajemen Berbasis Digital dalam UMKM: Sebuah Kajian Literatur. *Journal Of Human And Education (JAHE)*, *5*(2), 267–272. https://doi.org/10.31004/jh.v5i2.2340

Rahmawati, S., & Nasution, M. I. P. (2024). Evaluasi Implementasi Sistem Informasi Manajemen Berbasis Teknologi Cloud Computing pada Usaha Kecil dan Menengah (UKM). *Journal Of Informatics And Busisnes*, *2*(1), 37–41.

Rozi, F., Ibrahim, anton maulana, & Pujiastuti, E. (2024). Analisis Ancaman Keamanan dalam Penggunaan Teknologi Cloud Computing. *Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer*, *14*(3), 150–233. https://jurnal.umj.ac.id/index.php/just-it/index

Suartana, I. M., Putra, R. E., & Alit, R. (2024). Jurnal abadimas adi buana. *Jurnal Abadimas Adi Buana*, *7*(02), 279–286. https://jurnal.unipasby.ac.id/index.php/abadimas/article/view/8389

Ula, M., Adek, R. T., & Bustami, B. (2021). Perspektif Keamanan Pengguna Tentang Adopsi Dan Migrasi Teknologi Mobile Cloud. *Sisfo: Jurnal Ilmiah Sistem Informasi*, *5*(1), 92–105. https://doi.org/10.29103/sisfo.v5i1.4856