E-ISSN: 2407 - 3911
P-ISSN : 2686 - 0333

PENGEMBANGAN KEAMANAN CYBER PADA CLOUD COMPUTING UNTUK USAHA KECIL DAN MENENGAH

Muchamad Rusdan
Informatika
Sekolah Tinggi Teknologi Bandung
Jln. Soekarno-Hatta No.378, Kota Bandung 40235
rusdan@sttbandung.ac.id

Abstrak

Tujuan utama dari penelitian ini adalah untuk menguji strategi keamanan yang efektif untuk UKM pada teknologi *cloud computing*, dengan memeriksa ancaman keamanan untuk UKM, langkah-langkah mitigasi, dan strategi terbaik untuk keamanan yang efektif di lingkungan *cloud computing*. *Cloud computing* adalah paradigma yang relatif baru yang menghadirkan manfaat bisnis yang signifikan dan peluang yang sangat besar untuk usaha kecil dan menengah. Seiring berkembangnya teknologi informasi (TI), UKM perlu menemukan strategi yang efektif untuk memenuhi tuntutan bisnis. Namun, banyak UKM yang enggan mengadopsi teknologi cloud computing karena masalah keamanan, privasi, dan kepercayaan yang melekat, serta risiko regulasi dan implikasi kepatuhan. Penelitian terdahulu menunjukkan peningkatan jumlah serangan keamanan *cyber* yang menargetkan UKM di lingkungan *cloud*. Untuk mengatasi ancaman keamanan, ada kebutuhan untuk menetapkan praktik, standar, dan pedoman terbaik yang dapat diikuti oleh UKM. Penelitian ini membahas dua tujuan penelitian: (i) untuk mengidentifikasi ancaman keamanan dan tantangan yang dihadapi UKM di lingkungan *cloud* dan menentukan strategi mitigasi terbaik dan, (ii) untuk mengembangkan kerangka kerja strategi keamanan untuk UKM dalam konteks *cloud computing*. Kontribusi keseluruhan dari penelitian ini adalah model yang diusulkan, yang mengintegrasikan empat komponen strategis: Model *Cloud*, Model Keamanan, Model Kepatuhan, dan Komponen Keamanan Utama.

Kata kunci :

Keamanan *Cyber*, UKM, Komputasi Awan

Abstract

The main objective of this research is to test effective security strategies for SMEs on cloud computing technology, by examining security threats for SMEs, mitigation measures, and the best strategies for effective security in a cloud computing environment. Cloud computing is a relatively new paradigm that presents significant business benefits and enormous opportunities for small and medium businesses. As the information technology (IT) landscape develops, SMEs need to find effective strategies to meet business demands. However, many SMEs are reluctant to adopt cloud computing technology due to inherent security, privacy, and trust issues, as well as regulatory risks and compliance implications. Preliminary studies show an increasing number of cybersecurity attacks targeting SMEs in the cloud environment. To address security threats, there is a need to establish best practices, standards, and guidelines that can be followed by SMEs. This study addresses two research objectives: (i) to identify security threats and challenges facing SMEs in the cloud environment and determine the best mitigation strategies and, (ii) to develop a security strategy framework for SMEs in the context of cloud computing. The overall contribution of this research is the proposed model, which integrates four strategic components: the Cloud Model, the Security Model, the Compliance Model, and the Main Security Component.

Keywords :

Cyber Security, SME, *Cloud Computing*

I. PENDAHULUAN

Memasuki era globalisasi dan meningkatnya persaingan dalam konteks bisnis, organisasi perlu meningkatkan kompetensi inti mereka dan terus berevolusi untuk menahan tekanan persaingan yang semakin besar. Faktor-faktor seperti kendala anggaran dan langkah-langkah penghematan biaya memaksa perusahaan untuk mencari solusi alternatif untuk memenuhi persyaratan dan tujuan bisnis. Untuk Usaha Kecil dan Menengah (UKM), mencapai kesuksesan bisnis tetap menjadi tantangan (Hashemi & Hesarlo, 2014). Agar UKM dapat memenuhi kebutuhan pelanggan dan memberikan layanan yang lebih baik, mereka perlu menggunakan layanan Teknologi Informasi (TI). Namun, teknologi komputasi TI tradisional biasanya terbukti mahal bagi banyak UKM karena mereka tidak memiliki sumber daya dan kemampuan untuk mengintegrasikan dan mengelola teknologi ini walaupun, hubungan antara UKM dan inovasi TI biasanya saling menguntungkan. UKM membentuk elemen integral dari ekonomi suatu negara karena mereka berfungsi sebagai sumber lapangan kerja dan pendorong pengembangan teknologi. Kemajuan teknologi dan pengembangan solusi teknologi baru mendukung fungsi tersebut dan memberikan peluang bisnis yang sangat besar dan manfaat bagi UKM (Wang et al., 2011). Pemahaman umum adalah bahwa kemajuan dalam TI memberikan manfaat dan peluang penting bagi UKM untuk mencapai daya saing berdasarkan pada respons pelanggan yang lebih cepat, efisiensi dalam proses bisnis, dan pemasaran skala besar yang relatif murah.

Salah satu teknologi informasi yang relatif baru yang telah membawa peluang tambahan bagi perusahaan, adalah *cloud computing*. Menurut *National Institute of Standards and Technology* Amerika Serikat, *cloud computing* adalah paradigma komputasi yang melibatkan akses di mana saja dan sesuai permintaan ke sumber daya. Definisi ini mendukung lima fitur utama cloud computing, yaitu akses jaringan *broadband*, berbagi sumber daya, akses sesuai permintaan, elastisitas layanan, dan layanan yang terukur. Menurut Mell dan Grance (2011), *cloud computing* adalah arsitektur perangkat lunak dan perangkat keras yang memungkinkan skalabilitas, virtualisasi infrastruktur, dan penyedia layanan *cloud*. Dengan *cloud computing*, UKM tidak perlu menempatkan perangkat lunak dan *server* di lokasi perusahaan mereka atau bahkan mempekerjakan tenaga teknis untuk menjaga dan memelihara infrastruktur TI (Mohabbattalab, Heidt, dan Mohabbattalab, 2014). Daya tarik *cloud computing* terletak pada kemampuannya untuk memberikan UKM peluang untuk mengurangi biaya, meningkatkan produktivitas, dan meningkatkan respons layanan bisnis (Javaid, 2014).

Sementara *cloud computing* memberikan manfaat dan peluang bisnis yang signifikan, selain itu juga menghadirkan tantangan keamanan, privasi, dan kepercayaan, terutama untuk UKM (Hashemi & Hesarlo, 2014). Pada penelitian terdahulu menunjukkan peningkatan jumlah dan ukuran serangan cyber yang menargetkan UKM (Symantec, 2018). Ancaman dan serangan keamanan beragam dalam hal motivasi dan eksploitasi teknologi mulai dari serangan orang dalam yang dimotivasi oleh kejahatan hingga kesalahan konfigurasi jaringan perusahaan, kurangnya perencanaan keamanan, hingga eksploitasi otomatis dari kerentanan keamanan yang diketahui. Masalahnya adalah bahwa mengatasi tantangan privasi, kepercayaan, dan keamanan di lingkungan *cloud* tetap menjadi tantangan karena memerlukan kombinasi pendekatan organisasi, teknologi, dan hukum yang seringkali berada di luar kendali perusahaan.

Tujuan utama dari penelitian ini adalah untuk menguji strategi keamanan yang efektif untuk UKM pada teknologi *cloud computing*, dengan memeriksa ancaman keamanan terhadap UKM, langkah-langkah mitigasi, dan strategi terbaik untuk keamanan yang efektif pada lingkungan *cloud computing*. Saat ini, penelitian yang tersedia berfokus pada strategi keamanan untuk organisasi besar. Bahkan pendekatan tradisional penilaian risiko keamanan cenderung berfokus pada metode yang tidak sesuai dengan profil unik UKM dalam hal ketersediaan sumber daya dan kemampuan teknis. Hal tersebut menunjukkan perlunya penelusuran yang ekstensif untuk mengeksplorasi strategi terbaik bagi UKM dalam menggunakan layanan *cloud computing*.

II. KAJIAN LITERATUR

II.1 Definisi Keamanan *Cyber*

Sistem informasi dihadapkan pada berbagai ancaman keamanan *cyber*. Pada saat ini, organisasi berjuang dengan memahami ancaman apa yang ada untuk aset informasi dan bagaimana cara melawannya. Menurut Fischer (2016), risiko yang

terkait dengan serangan *cyber* tergantung pada tiga faktor yang saling terkait yaitu, ancaman, kerentanan, dan dampak. Ancamannya adalah orang atau sistem yang memulai serangan *cyber*.

Dengan kemajuan teknologi informasi (TI) seperti *internet* dan paradigma *mobile cloud computing* (MCC), fokus telah diarahkan untuk melindungi sistem informasi dari serangan *cyber*. Akibatnya, keamanan *cyber* terus mendapat perhatian ilmiah yang tinggi karena para pakar industri memperkirakan jumlah serangan *cyber* dan tingkat serangan semakin meningkat di masa depan (Verizon, 2016). Sementara teknologi informasi telah menjadi aspek yang tak terpisahkan dari masyarakat modern dan membawa implikasi keamanan yang penting. Dalam lingkungan bisnis modern, teknologi seperti *cloud computing*, *mobile computing*, dan *social computing* secara signifikan mengubah cara perusahaan menggunakan TI untuk melakukan perdagangan online dan berbagi informasi. Untuk menjaga kerahasiaan, integritas, dan ketersediaan data, organisasi banyak berinvestasi dalam sumber daya teknologi dan jam kerja untuk menciptakan tindakan pencegahan (Vinnakota, 2013).

Pada penelitian Goutam (2015), menjelaskan bahwa keamanan *cyber* sebagai teknologi dan proses yang dirancang untuk melindungi komputer dan jaringan komputer dari akses yang tidak sah. Demikian pula, *International Telecommunications Union* (ITU), mendefinisikan bahwa keamanan *cyber* sebagai kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang digunakan untuk melindungi lingkungan *cyber* (ITU, nd). Sifat *cyber space* yang tanpa batas dan ada di mana-mana menciptakan *platform* yang mendorong anonimitas dan memfasilitasi perilaku kriminal, termasuk berbagai bentuk serangan *cyber*, *cyberbullying*, pencurian kekayaan intelektual (IP), dan pencurian identitas. Menurut Bendovschi (2015), karakteristik kritis dari sebuah perusahaan modern meliputi penggunaan jaringan sosial yang luas, data besar, transaksi online, dan informasi luas yang disimpan dan dikelola melalui proses otomatis. Keamanan informasi dan privasi data adalah risiko permanen dan terus berkembang dalam lingkungan seperti itu.

Menurut *Symantec Security Threat Report* untuk tahun 2018, lebih dari 430 juta ancaman *malware* unik ditemukan pada 2017, mewakili peningkatan 36% dari tahun sebelumnya (Symantec, 2018). Laporan tersebut menunjukkan bahwa serangan yang menargetkan organisasi dan bisnis secara umum terus meningkat. Namun, wawasan paling penting dari data yang tersedia adalah evolusi serangan *Web*, *toolkit*, dan eksploitasi kerentanan *online*.

Masih menurut Symantec (2018), penyerang mengeksploitasi setiap kerentanan yang mereka temukan dan kompromi situs *web* untuk memerintah *server host*. Tren ini menunjukkan semakin besarnya kerentanan bisnis terhadap berbagai serangan keamanan dan pelanggaran data dengan implikasi ekonomi yang signifikan. Menurut laporan tersebut, sebagian besar serangan saat ini menargetkan perangkat mobile dan *Internet of Things* (IoT), ancaman web, ancaman media sosial dan email, layanan dan infrastruktur *cloud computing*, serta serangan bertarget, *phishing*, dan pencurian kekayaan intelektual di antara bentuk lain dari pelanggaran data dan pelanggaran privasi (Symantec, 2018).

II.2 Definisi Usaha Kecil dan Menengah (UKM)

Saat ini, tidak ada definisi spesifik dari istilah UKM yang dapat diambil sebagai referensi untuk semua negara. Akibatnya, berbagai negara memiliki kriteria yang berbeda untuk mendefinisikan UKM. Namun, meskipun tidak ada definisi universal, pentingnya definisi tersebut tidak dapat disangkal. Menurut Lucky (2012), kriteria umum untuk mendefinisikan UKM termasuk ukuran organisasi, jumlah karyawan, ukuran industri, dan nilai aset. Demikian pula, Komisi Perdagangan Internasional AS (2010) mengakui jumlah karyawan dan pendapatan tahunan sebagai kriteria klasifikasi dasar. *Small Business Administration* (SBA) (2017) belum memberikan definisi langsung tentang UKM karena mencakup semua bisnis dengan kurang dari 500 karyawan. Definisi ini akan berlaku untuk sisa penelitian ini. Secara umum, sektor UKM terdiri dari tiga kategori usaha: usaha mikro, usaha kecil, dan usaha menengah atau usaha. Perusahaan mikro adalah yang terkecil dari tiga kategori, yang terdiri dari hingga sembilan karyawan. Bisnis menengah adalah yang terbesar di antara kategori UKM dalam hal jumlah karyawan, dan investasi modal. Tiga kategori termasuk dalam deskripsi SBA dan akan menjadi bagian dari definisi yang digunakan dalam penelitian ini.

II.3 Ancaman Keamanan TI Pada UKM

Cybercrime Survey (2013) menunjukkan meningkatnya ancaman serangan *cyber* kepada UKM. Laporan tersebut menunjukkan bahwa kerentanan TI paling umum yang mempengaruhi UKM termasuk kolaborasi sosial, merangkul mobilitas tenaga kerja dan peningkatan penggunaan perangkat *mobile*, penyimpanan *cloud*, dan digitalisasi informasi privasi. Agensi yang berfokus pada masalah yang mempengaruhi UKM telah mempublikasikan daftar ancaman keamanan TI paling umum yang dihadapi bisnis di AS. Ada sumber valid lain ancaman keamanan TI seperti Laporan Pelanggaran Data Verizon (2016) memberikan laporan kejadian untuk berbagai jenis bisnis termasuk UKM dan perusahaan besar. Demikian pula, Symantec (2018) *Internet Security Threat Report* memberikan tinjauan mendalam dan analisis kegiatan ancaman keamanan global untuk semua jenis bisnis.

Untuk mendapatkan gambaran lengkap tentang ancaman yang dihadapi UKM, penting untuk menganalisis laporan keamanan *cyber* yang ada dan menghasilkan pandangan komprehensif tentang postur keamanan perusahaan. Diskusi dari masing-masing ancaman keamanan terdiri dari definisi, aset TI di bawah ancaman, dan langkah-langkah mitigasi yang mungkin dilakukan oleh UKM. Ancaman keamanan paling umum yang dihadapi UKM menurut laporan tersebut adalah ancaman orang dalam, kurangnya perencanaan kontingensi, konfigurasi jaringan yang buruk, dan penggunaan jaringan Wi-Fi yang tidak aman, perangkat mobile, kompromi *server web*, email HTML, dan eksploitasi kerentanan (WatchGuard 2008).

II.4 Definisi *Cloud Computing*

Istilah *cloud computing* berasal dari berbagai perspektif di bidang akademis dan praktik, yang menjelaskan variasi dalam definisi. Buyya et al. (2009) menggambarkan *cloud computing* sebagai 'utilitas kelima' bersama dengan air, gas, listrik, dan telepon. Berdasarkan uraian ini, *cloud computing* mencakup akses yang tersedia dan sesuai permintaan ke layanan komputasi seperti utilitas lainnya. NIST memberikan definisi dari *cloud computing* dengan menggambarkannya sebagai sebuah model untuk memungkinkan akses jaringan di mana saja, nyaman, sesuai permintaan ke kumpulan sumber daya komputasi yang dapat dikonfigurasi serta dapat dibagi. Penelitian ini akan menggunakan definisi ini karena menggambarkan model *cloud* menggunakan lima karakteristik penting, tiga model layanan, dan empat jenis model penyebaran.

Pada dasarnya, definisi NIST untuk *cloud computing* membedakan lima karakteristik utama dari model *cloud*: layanan mandiri *ondemand*, akses jaringan luas, pengumpulan sumber daya, elastisitas cepat, dan layanan terukur (Mell & Grance, 2011). Setiap layanan *cloud computing* perlu mendukung karakteristik kunci ini. Di sisi lain, NIST mengidentifikasi tiga jenis model layanan *cloud*: Software as a Service (SaaS), Platform as a Service (PaaS), dan Infrastructure as a Service (IaaS). SaaS menjelaskan kemampuan bagi konsumen untuk menggunakan aplikasi yang disediakan oleh penyedia *cloud* dari berbagai perangkat klien dan antarmuka program. PaaS menjelaskan kemampuan bagi konsumen untuk menyebarkan aplikasi yang diperoleh atau dibuat menggunakan berbagai bahasa pemrograman, alat, dan layanan ke infrastruktur *cloud*. Terakhir, IaaS menjelaskan kemampuan bagi konsumen untuk menyediakan penyimpanan, pemrosesan, jaringan, dan sumber daya komputasi lainnya untuk menyebarkan dan menjalankan perangkat lunak termasuk OS dan aplikasi. Terlepas dari tiga model layanan *cloud* utama, model tambahan telah dijelaskan dalam literatur termasuk *Desktop-as-a-Service* (DaaS), dan *Database-as-a-Service* (DBaaS), keduanya adalah himpunan bagian dari PaaS yang menggambarkan kemampuan untuk pengguna dapat meminta layanan basis data menggunakan portal.

NIST menjelaskan empat jenis model penyebaran tergantung pada hubungan antara penyedia layanan *cloud* yaitu, *private cloud*, *community cloud*, *public cloud*, dan *hybrid cloud*. Keamanan dan privasi model-model ini bervariasi sesuai dengan penyebarannya.

II.5 Masalah dan Tantangan Keamanan *Cloud*

Untuk bisnis, *cloud computing* hadir dengan kemungkinan dan tantangan yang sangat besar. Selain ketersediaan dan kepercayaan, keamanan dan privasi tetap menjadi tantangan paling signifikan bagi perusahaan. Memang, berbagai kelemahan dalam arsitektur *cloud* menciptakan kerentanan terhadap ancaman keamanan dan privasi. Menurut Nazir dan Rashid (2013), masing-masing dari tiga model penyebaran *cloud* menyajikan kelebihan dan kekurangan yang unik dalam hal keamanan dan

privasi. Masalah keamanan utama dalam *cloud* publik termasuk kurangnya kontrol atas siklus data, kurangnya kepastian ketersediaan sistem dan cadangan data, dan aplikasi *multi-tenancy*, yang meningkatkan kerentanan (Nazir dan Rashid, 2013). Model *cloud* pribadi memungkinkan pelanggan untuk membangun kendali atas jaringan tetapi penggunaan umum dari teknik virtualisasi memperkenalkan kerentanan tambahan. Selain ancaman reguler terhadap keamanan jaringan terdapat tujuh masalah utama yang terkait dengan *cloud computing* seperti kehilangan data, pelanggaran data, orang dalam yang jahat, antarmuka yang tidak aman, lokasi data, peretasan layanan, dan *denial of service* (DoS).

III. HASIL DAN PEMBAHASAN

Studi ini menunjukkan berbagai temuan utama yang memiliki implikasi pada UKM yang berupaya mengadopsi cloud computing. Secara khusus, temuan penelitian menunjukkan bahwa adopsi *cloud* computing oleh UKM tergantung pada faktor-faktor seperti konteks organisasi, konteks teknologi, dan konteks lingkungan. Teknologi baru diharapkan akan membawa manfaat dan nilai tambahan bagi bisnis. Namun, UKM mungkin menunda pengadopsian teknologi baru karena risiko yang dirasakan seperti ancaman keamanan dan privasi, kehilangan kendali, dan pemahaman yang buruk tentang manfaat penggunaan *cloud computing*.

III.1 Ancaman dan Risiko Keamanan *Cloud Computing* Pada UKM

Secara keseluruhan, masalah keamanan yang dihadapi UKM di lingkungan *cloud* termasuk dalam lima kategori, masalah jaringan, masalah standar keamanan, masalah infrastruktur *cloud*, masalah kontrol akses, dan masalah data. Masalah yang berhubungan dengan jaringan termasuk ancaman yang ditimbulkan oleh serangan DoS dan DDoS, serangan *man in the middle* (MITM), serangan *flooding*, serangan DNS, dan kerentanan IP. Ada juga kekhawatiran tentang ketergantungan pada *Internet* dan konfigurasi keamanan jaringan. Masalah keamanan termasuk kurangnya standar keamanan yang memadai untuk memastikan keamanan yang kuat untuk perusahaan, masalah kepercayaan saat bekerja melalui *Internet*, dan masalah kepatuhan. Literatur yang ada lebih berfokus pada standar yang tersedia yang diperlukan untuk mengurangi serangan *cyber* di infrastruktur cloud dan kebijakan yang dapat melindungi dari sistem *cloud*. Untuk infrastruktur *cloud*, masalah keamanan utama untuk UKM termasuk antarmuka API yang tidak aman, kesalahan konfigurasi keamanan, lokasi *server* dan cadangan data, serta karakteristik *multi-tenancy* dari lingkungan *cloud*. Tema kontrol akses menyinggung berbagai masalah keamanan seperti orang dalam yang jahat, mekanisme otentikasi, pembajakan akun dan layanan, dan akses pengguna istimewa. Dampak ini unik untuk setiap bisnis. Terakhir, UKM juga memiliki masalah keamanan umum tentang perlindungan data, integritas, ketersediaan, dan risiko kehilangan data dan masalah privasi sehingga diperlukan solusi *multi-level*.

Analisis lebih lanjut dari literatur yang ada mengidentifikasi 11 ancaman keamanan prioritas yang dihadapi UKM di cloud. Ancaman keamanan pertama adalah kerentanan keamanan perangkat lunak seperti layanan email SaaA, yang rentan terhadap injeksi SQL. Fitur *multi-tenancy* dari lingkungan cloud membuat pelanggan terkena serangan yang berupaya mengeksploitasi kegagalan isolasi. Hal tersebut menyiratkan bahwa UKM perlu menggunakan isolasi sumber daya yang efektif dan isolasi *cache virtual*. Meskipun demikian, *cloud* pribadi akan sesuai untuk UKM karena menyediakan fitur keamanan yang kuat terlepas dari implikasi biaya yang harus dikeluarkan. Ancaman prioritas kedua bagi UKM adalah serangan jaringan. Menggunakan koneksi Internet membuat UKM menghadapi risiko besar yang terkait dengan MITM, *network traffic sniffing*, dan serangan DoS. Dikombinasikan dengan masalah konfigurasi jaringan yang terkait dengan jaringan UKM, risiko menjadi semakin jelas. Untuk UKM, ini menyiratkan kebutuhan untuk fokus pada melindungi data di sisi *server*, sisi klien, dan mengurangi serangan yang mengekspos layanan penyimpanan *cloud*. Risiko keamanan prioritas lainnya termasuk serangan *social engineering*. API compromise dan kerentanan terhadap manajemen GUI, pencurian perangkat, *overloads*, penguncian vendor, biaya tak terduga, masalah hukum, dan pemadaman administrasi.

III.2 Tindakan Mitigasi untuk Ancaman Keamanan *Cloud Computing* Pada UKM

Untuk mengatasi tujuan penelitian kedua, penelitian ini memeriksa standar praktik keamanan *cyber* saat ini, dan langkah-langkah, teknik mitigasi ancaman terhadap masalah keamanan dalam konteks *cloud computing*, dan pendekatan untuk manajemen

risiko keamanan *cloud*. Sejak awal, temuan penelitian menunjukkan bahwa metode keamanan yang paling umum digunakan oleh perusahaan termasuk *firewall*, pemisahan jaringan fisik, mekanisme kontrol akses berbasis peran, enkripsi data, dan manajemen identitas, serta pemantauan media cadangan. Pada penelitian ini menemukan bahwa UKM menggunakan alat keamanan seperti teknologi *firewall, security intelligence systems*, alat tata kelola akses, kontrol perimeter, dan alat untuk manajemen kebijakan otomatis. Sementara tidak ada jalan pasti untuk berhasil dalam penerapan langkah-langkah keamanan, temuan menunjukkan kematangan dalam hal praktik keamanan dan standar yang dirancang untuk memandu perusahaan. Contoh praktik terbaik dan panduan termasuk Kerangka Keamanan *Cyber* NIST, standar ISO / IEC 27000, dan *Critical Security Controls* (CIS).

Untuk mengurangi ancaman keamanan pada *cloud*, penelitian ini menetapkan perlunya bagi UKM untuk fokus pada manajemen risiko. Penelitian ini menetapkan bahwa UKM semakin menyadari pentingnya manajemen risiko, tetapi manajemen risiko yang efektif tetap menjadi tantangan bagi banyak bisnis. Masalahnya adalah bahwa pendekatan tradisional untuk manajemen risiko cenderung fokus pada mengadopsi metodologi umum yang menangani risiko untuk semua jenis organisasi. Mengingat sifat unik dari UKM dalam hal postur keamanan mereka, metodologi ini akan terlalu rumit dan tidak cocok. Namun, analisis lebih lanjut telah mengidentifikasi metodologi *CloudWatch2* sebagai alat yang sesuai untuk UKM. *CloudWatch* dibenarkan karena menyediakan pendekatan yang disederhanakan dan mudah untuk penilaian risiko pada *cloud*. Untuk UKM, kesesuaian CloudWatch memungkinkan untuk dapat menilai postur keamanan UKM, memilih kontrol keamanan yang sesuai, serta menyebarkan dan memantau *risk profile*.

III.3 Mengembangkan Model Keamanan *Cloud* untuk UKM

Setelah memahami ancaman keamanan, risiko, dan tantangan umum bagi UKM pada *cloud* dan memetakan langkah-langkah mitigasi keamanan, langkah selanjutnya untuk penelitian ini adalah mengembangkan strategi untuk penerapan *cloud* yang efektif dan aman untuk UKM. Strategi ini direpresentasikan sebagai kerangka kerja konseptual yang dimodelkan menggunakan Arsitektur Keamanan Konseptual SABSA (Sherwood et al., 2009). Model konseptual yang diusulkan mengintegrasikan empat komponen: *Cloud Model, Security Model, Compliance Model,* dan *Security Major*.

Cloud Model adalah langkah pertama dalam strategi keamanan keseluruhan untuk UKM, dan ini menjawab pertanyaan "Apa" yang harus dilindungi dan "Siapa" yang akan terlibat dalam manajemen keamanan perusahaan. Untuk UKM yang berupaya menggunakan teknologi *cloud computing*, langkah pertama dalam strategi penyebaran *cloud* yang dipertimbangkan dalam model ini adalah mengidentifikasi tipe sistem yang akan digunakan dan menentukan siapa yang akan menggunakan sistem. Pendekatan ini memungkinkan UKM untuk memetakan arsitektur keamanan dan menentukan persyaratan bisnis, peraturan, dan kepatuhan. Model ini mengidentifikasi berbagai sumber ancaman dalam *cloud computing*, termasuk aktor *cloud*, model penyebaran *cloud*, dan model layanan *cloud*.

Model Keamanan, yang sesuai dengan langkah kedua dari strategi *cloud* UKM. Langkah ini membahas pertanyaan "Mengapa" perlindungan akan dibutuhkan di lingkungan *cloud* dan "Di mana" UKM ingin mencapai perlindungan. Agar UKM dapat menjawab pertanyaan "Mengapa", mereka perlu fokus pada risiko penyebaran aset informasi, data, dan aplikasi mereka di setiap model *cloud computing* dan model penyebaran. Model Keamanan memberikan Model Matriks Risiko yang direpresentasikan sebagai berikut:

RMM = BARE x CCTT

Dimana:
RMM = *Risk Matrix Model*
BARE = *Bank Asset Risk Exposure*
CCTT = *Cloud Computing Top Threat*

Model Matriks Risiko mengikuti definisi ISO-27001 tentang *risk exposure*. Ini berarti bahwa pemilik bisnis perlu mengidentifikasi aset tertentu dan ancaman keamanan teratas terhadap *cloud computing* untuk melakukan pengukuran risiko. Setelah mengukur risiko keamanan, para pihak perlu menentukan di mana harus menerapkan kontrol. Konsep paling penting untuk dipertimbangkan di sini termasuk domain keamanan *logical* dan *physical* serta batas domain terkait. Model ini membayangkan tiga jenis domain kontrol yaitu, teknis, administratif, dan fisik. Selain itu, model memetakan kontrol ini untuk setiap komponen sumber daya *cloud computing*.

Komponen ketiga adalah Model Kepatuhan, dan membahas pertanyaan tentang bagaimana UKM ingin mencapai perlindungan yang mereka butuhkan pada lingkungan *cloud*. Komponen terakhir adalah Arsitektur Keamanan. Agar UKM dapat mencapai keamanan yang efektif dalam *cloud computing*, mereka perlu mempertimbangkan komponen arsitektur *cloud* dan kontrol yang memenuhi standar internal.

IV. KESIMPULAN DAN SARAN

IV.1 Kesimpulan

Pada penelitian ini telah mengeksplorasi strategi yang efektif untuk keamanan UKM dalam *cloud* computing. Penelitian ini telah menyelidiki tantangan keamanan yang dihadapi UKM pada *cloud*, termasuk ancaman dan risiko keamanan utama, serta langkah-langkah mitigasi, praktik terbaik, dan standar terbaik. Dengan mengadopsi kerangka kerja konseptual, temuan penelitian ini mendukung gagasan bahwa berbagai faktor mempengaruhi strategi yang digunakan UKM untuk mengadopsi *cloud computing*. Lebih penting lagi, kerangka kerja yang diusulkan ini berasal dari gagasan bahwa tidak ada satu jalan menuju kesuksesan untuk keamanan *cloud* UKM. Sebaliknya, kerangka kerja ini menggambarkan konteks yang berbeda dalam hal ancaman keamanan, kerentanan, dan postur risiko umum. Dengan demikian, model mengantisipasi variasi dalam strategi yang diadaptasi oleh UKM untuk mengamankan aset pada *cloud*. Model ini menyediakan kerangka kerja fleksibel yang dapat memandu UKM untuk memilih langkah-langkah keamanan, kebijakan, dan strategi terbaik berdasarkan keadaan keamanan unik di cloud. Direkomendasikan bahwa UKM menggunakan model yang diusulkan sebagai panduan untuk mengamankan informasi dan aset lainnya ketika pindah ke solusi *cloud* apa pun.

IV.2 Saran

Studi ini memiliki implikasi penting bagi pemilik UKM, vendor perangkat lunak *cloud*, dan konsultan teknologi. Untuk pemilik bisnis, penelitian ini memberikan tinjauan umum tentang risiko keamanan dan menyediakan model untuk menemukan tindakan pencegahan terbaik. Karena UKM mewakili mayoritas bisnis di banyak negara, UKM juga mewakili segmen ekonomi yang signifikan untuk penyedia layanan dan vendor perangkat lunak. Sebagian besar ketidakpastian yang ada seputar *cloud computing* untuk UKM adalah bagaimana data ditangani dalam lingkungan *cloud* tanpa memperhatikan aset bisnis penting lainnya. Penelitian ini bertujuan untuk mengetahui tentang strategi yang dapat digunakan oleh UKM untuk meningkatkan keamanan di *cloud*. Sementara penelitian telah memenuhi maksud dan tujuan penelitian, ada berbagai bidang untuk penelitian tambahan mengingat keterbatasan penelitian. Harus diakui, penelitian ini mewakili sebagian kecil dari literatur yang luas tentang strategi keamanan untuk keberhasilan UKM dalam *cloud computing*. Namun, seperti disebutkan sebelumnya, ada kurangnya penelitian tentang strategi keamanan spesifik yang dapat digunakan oleh UKM untuk mencapai keberhasilan dalam *cloud computing* meskipun ada ancaman keamanan yang terdokumentasi dengan baik. Penelitian di masa depan dapat memperluas temuan penelitian dengan memvalidasi model yang diusulkan dan memeriksa strategi yang tepat untuk *cloud computing* di berbagai sektor, industri, atau negara.

REFERENSI

Bendovschi, A 2015, 'Cyber-attacks: trends, patterns, and security countermeasures' 7th International Conference on Financial Criminology, Procedia Economics and Finance, vol. 28, pp. 24-31.

Buyya, R. Yeo, CS. Venugopal, S. Broberg, J & Brandic, I 2009, 'Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility', Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616.

Fischer, EA 2016, 'Cybersecurity issues and challenges: In brief. Congressional Research Service (7-5700 R43831)'.

Goutam, RK 2015, 'Importance of cybersecurity', International Journal of Computer Applications, vol. 111, no.7, pp. 14-17.

Lucky, EO 2012, 'Is Small and Medium Enterprise (SME) an entrepreneurship', International Journal of Academic Research in Business and Social Sciences, vol. 2, no. 1, pp. 341-352.

Mell, P & Grance, T 2011, September, 'The NIST definition of cloud computing', NIST Special Publication 800-145.

Mohabbattalab, E. Heidt, T & Mohabbattalab, B 2014, 'The perceived advantages of cloud computing for SMEs', GSTF Journal on Computing, vol. 4, no. 1, pp. 61-65.

Nazir, M & Rashid, MS 2013, 'Security threats with associated mitigation techniques in cloud computing', International Journal of Applied Information Systems, vol. 5, no. 7, pp. 16-27.

Sherwood, J. Clark, A & Lynas, D 2009, 'SABSA: Enterprise security architecture', SABSA, White Paper, Sabsa Limited.

Symantec, 2018, 'Internet Security Threat Report'. Available from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2018-en.pdf. [24 Nopember 2019].

Verizon.com, 2016 'Data Breach Investigations Report'.

Vinnakota, T 2013, 'Understanding of cyberspace using cybernetics: an imperative need for cybersecurity of enterprises', IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), pp. 107-111.

Wang, R. Von, G. Younge, A. He, X. Kunze, M. Tao, J & Fu, C 2010, 'Cloud computing: a perspective study', New Generation Computing, vol. 28, no. 2, pp. 137-146.

WatchGuard.com, 2008, 'Top 10 Threats to SME Data Security'.