KERANGKA KAWALAN CAPAIAN BERASASKAN RISIKO DENGAN POLISI KAWALAN TERLINDUNG DALAM PENGKOMPUTERAN AWAN

SALASIAH BINTI ABDULLAH

UNIVERSITI KEBANGSAAN MALAYSIA

KERANGKA KAWALAN CAPAIAN BERASASKAN RISIKO DENGAN POLISI KAWALAN TERLINDUNG DALAM PENGKOMPUTERAN AWAN

SALASIAH BINTI ABDULLAH

DISERTASI YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEH
IJAZAH SARJANA SISTEM MAKLUMAT

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA

2019

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

17 Januari 2019

SALASIAH BINTI ABDULLAH
P87559

PENGHARGAAN

Pertama sekali saya ingin memanjatkan kesyukuran kepada Allah Taala atas kekuatan yang dikurniakan kepada saya sepanjang perjalanan melengkapkan program sarjana ini. Saya mengucapkan terima kasih kepada Dr. Khairul Azmi Bin Abu Bakar selaku penyelia yang telah memberikan tunjuk ajar dan bimbingan.

Terima kasih khas ditujukan kepada suami, Mohd Nurakmal Bin Nasir serta anak-anak, Dhia Aryssa Mohd Nurakmal dan Aina Safiyya Mohd Nurakmal kerana memberikan sokongan dan berkorban masa demi memastikan pengajian sarjana saya sampai ke penghujungnya.

Ucapan terima kasih tidak terhingga untuk emak, Supiyati Binti Mat Sileh dan ayah, Abdullah bin Senong serta keluarga dan kawan-kawan yang banyak memberikan bantuan, dorongan dan kata-kata semangat sepanjang pengajian ini. Semoga anda semua dalam rahmat Allah dan dipermudahkan urusan dunia akhirat.

ABSTRAK

Kemunculan pengkomputeran awan telah memperkasakan sistem perhubungan dan komunikasi sekaligus menyokong peralihan data dan peranti fizikal kepada persekitaran maya. Walau bagaimanapun, ancaman keselamatan dan privasi telah dikenalpasti sebagai cabaran dalam menyokong tahap penggunaan awan di kalangan pengguna dan meningkatkan keperluan dalam melindungi awan dengan pelaksanaan kawalan capaian yang dinamik. Justeru, pengenalan model *Risk Adaptable Access Control (*RAdAC*)* sebagai medium yang fleksibel berupaya mengendalikan permintaan capaian yang tersendiri dengan penguatkuasaan polisi risiko berdasarkan nilai atribut dan konteks semasa pengguna. Walau bagaimanapun, aspek perlindungan identiti pengguna dalam model RAdAC sedia ada tidak dibincangkan secara mendalam dalam kajian terdahulu. Kajian ini membincangkan tentang konsep asas dalam senibina pengkomputeran awan sekaligus mengenalpasti isu dan keperluan keselamatan serta cabaran awan. Dalam kajian ini, analisa perbandingan berpandukan elemen penting dalam kerangka RAdAC sedia ada telah dirumuskan dan elemen perlindungan privasi pengguna telah dikenalpasti sebagai jurang kajian. Justeru, kaedah kualitatif yang dilaksanakan merangkumi kajian teoritikal berdasarkan sorotan kajian kepustakaan serta kajian empirikal berdasarkan temubual separa berstruktur bersama pegawai dengan kepakaran teknikal dalam keselamatan IT. Seterusnya, dapatan hasil kajian teoritikal dan empirikal telah dianalisa dengan menggunakan teknik analisis kandungan dan analisa keselamatan tidak formal. Sembilan komponen keselamatan telah dikenalpasti iaitu kebolehpercayaan, keselamatan data, integriti data, capaian data, pengesahihan, ketersediaan, kerahsiaan data, pengurusan identiti pengguna serta tidak boleh disangkal dalam pengkomputeran awan. Hasil penilaian pakar telah digunakan untuk mencadangkan pembangunan kerangka kerangka kawalan capaian berasaskan risiko dengan polisi kawalan terlindung (RiHAP). Kesimpulannya, kajian ini melibatkan penambahbaikan model kawalan capaian berasaskan risiko sedia ada dengan integrasi Protokol *Oblivious Commitment Based Envelope* (OCBE) dalam pelaksanaan polisi kawalan terlindung. Justeru, risiko pendedahan maklumat dapat diminimumkan untuk membenarkan awan menjalankan fungsi sebagai hab storan maklumat digital.

FRAMEWORK OF RISK BASED ACCESS CONTROL WITH HIDDEN ACCESS POLICY IN CLOUD COMPUTING.

ABSTRACT

The emergence of pervasive cloud computing has supported the transition of physical data and machine into virtualization environment. However, security threat and privacy have been identified as a challenge to support the widespread adoption of cloud among user and increased the needs to safeguard the cloud by implementing dynamic access control. Therefore, the emergence of Risk-Adaptable Access Control (RAdAC) has been identified as a flexible medium in handling exceptional access request and reacting to suspicious user by enforcing risk policies. However, the rising problem in safeguarding users' privacy in RAdAC model has not been discussed in depth by other researcher. This paper explores the fundamental concept of cloud computing architecture and identifies the security issues, requirements and challenges in cloud. In this work, the prerequisite elements in existing RAdAC framework has been discussed precisely and ambiguity factor is found in protecting privacy of user. Thus, qualitative method has been conducted throughout the research involving theoretical study on literature review and empirical analysis on semi structured interview with IT security practitioners. Next, the findings from both theoretical and empirical study have been emphasized using content analysis technique and informal security analysis. Nine security components have been identified which are reliability, data security, data integrity, data access, authentication, availability, confidentiality of data, user identity management and non-repudiation in cloud computing. Finally, experts validation demonstrate that the proposed Risk Based Access Control with Hidden Access Policy (RiHAP) framework with the integration of *Oblivious Commitment Based Envelope* (OCBE) protocol significantly impact the minimization of security exposure risk to serve as digital information storage hub.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

ABAC	Kawalan Capaian Berasaskan Atribut
ACL	Access Control List
CIO	Ketua Pegawai Maklumat
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CSP	Cloud Service Provider
HASBE	Hierarchical Attribute-Set-Based Encryption
IaaS	Infrastructure as a Service
IBAC	Kawalan Capaian Berasaskan Identiti
IdP	Identity Provider
KP-ABE	Key-Policy ABE
LDAP	Lightweight Directory Access Protocol
MFT	Managed File Transfer
NIST	National Institute of Standards and Technology
OCBE	Oblivious Commitment Based Envelope
PaaS	Platform as a Service
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PII	Maklumat Pengecaman Individu
RAdAC	Risk Adaptable Access Control
RADAM	Risk Adaptive Authorization Mechanism
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
RBAC	Kawalan Capaian Berasaskan Peranan
RiHAP	Kawalan Capaian Berasaskan Risiko dengan Polisi Kawalan Terlindung
SaaS	Software as a Service
SHA-2	Secure Hash Algorithm-2

BAB I

PENDAHULUAN

1.1 PENGENALAN

Penghasilan dokumen yang meningkat dari sehari ke sehari telah menyebabkan anjakan kehendak pengguna terhadap peningkatan keupayaan storan dan keselamatan dokumen. Justeru, pengkomputeran awan merupakan platform terbaik bagi memenuhi kehendak pengguna dalam menyediakan storan tanpa had dan menawarkan capaian data yang selamat melalui rangkaian pelayan maya yang dihoskan di internet.

Selain itu, pengkomputeran awan telah memberi impak yang besar dalam meningkatkan perkongsian maklumat antara pengguna dari lokasi geografi yang berbeza. Bukan itu sahaja, pengguna berpeluang mengakses awan dan berkongsi dokumen tanpa had sempadan dan sekatan rangkaian komputer. Justeru, pengkomputeran awan berupaya mengubah hala tuju persekitaran teknologi maklumat daripada pengurusan storan fizikal oleh pengguna kepada pengurusan sumber secara maya oleh awan. Namun, aspek keselamatan komputer dan privasi merupakan cabaran terbesar dalam pengkomputeran awan apabila migrasi sumber daripada storan fizikal kepada storan maya menyebabkan pengguna hilang kawalan sepenuhnya ke atas data storan (Wei et al. 2014). Hal ini menjurus kepada persoalan pengguna tentang kredibiliti awan dalam menguruskan sumber secara selamat dan berkesan.

Dalam menangani aspek keselamatan dan privasi dalam pengkomputeran awan, sesuatu sistem itu perlu berupaya mengawal akses dan capaian kepada sumber ataupun data. Selain itu, aplikasi sistem kawalan capaian yang berkesan mampu melindungi sumber dan maklumat penting bergantung kepada penetapan polisi kawalan keselamatan.

Kamus Pelajar Edisi Kedua Dewan Bahasa Dan Pustaka mendefinisikan capaian sebagai proses memasuki ruangan simpanan untuk menyimpan atau mendapatkan kembali data dalam komputer (Dewan Bahasa Pustaka 2016). Justeru, sistem kawalan capaian secara berkesan berupaya memastikan pengurusan proses kebenaran capaian berjalan dengan lancar dan sistematik.

Oleh sebab itu, kawalan capaian merupakan faktor penting dalam menangani cabaran pengkomputeran awan dengan penawaran fungsi kebenaran atau penafian akses pengguna bagi menjamin kerahsiaan data serta melindungi maklumat daripada pengguna hasad ataupun ancaman luar yang berniat jahat. Selain itu, kawalan capaian ialah mekanisma yang terbaik dalam menguatkuasakan polisi keselamatan dokumen dalam awan yang bertindak sebagai data storan. Pelbagai kaedah kawalan capaian telah dicadangkan dalam kajian lepas seperti *Access Control List* (ACL), Kawalan Capaian Berasaskan Peranan (RBAC), Kawalan Capaian Berasaskan Atribut (ABAC) dan *Risk Adaptable Access Control* (RAdAC). Setiap kawalan capaian tersebut mempunyai kekuatan dan kelebihan tersendiri dalam melengkapi persekitaran awan yang kondusif.

Justeru, setiap organisasi yang mengendalikan awan bebas untuk menentukan kaedah kawalan capaian yang sesuai berdasarkan kepada keperluan sistem dan tahap keselamatan dokumen masing-masing. Walau bagaimanapun, kebanyakan model kawalan capaian yang dibangunkan pada masa kini adalah menjurus kepada keperluan keselamatan komputer yang tinggi serta persekitaran yang dinamik. Kajian yang dijalankan oleh Karp et al. (2010) serta Mulimani & Rachh (2016) ke atas pelbagai kaedah kawalan capaian yang sedia ada telah membuktikan bahawa keberkesanan model kawalan capaian adalah bergantung kepada keupayaan model yang mampu berfungsi secara dinamik serta menawarkan perlindungan maklumat dan identiti pengguna secara berkesan.

Selain itu, evolusi dalam pembangunan kaedah kawalan capaian yang dijalankan oleh penyelidik terdahulu telah meningkatkan potensi pembangunan model RAdAC yang berkesan. Justeru, kajian ini mengaplikasikan konsep RAdAC dan terfokus kepada keberkesanan kerangka kawalan capaian berasaskan risiko yang berkesan dengan integrasi polisi kawalan terlindung dalam pengkomputeran awan.

Konsep RAdAC (Britton & Brown 2007) telah digunakan untuk menangani risiko keselamatan dan keperluan operasi dalam mengendalikan perkongsian dan transaksi maklumat. Kawalan capaian berasaskan risiko ini dicadangkan berdasarkan keupayaannya menampung keperluan fleksibiliti dalam persekitaran pengkomputeran awam yang dinamik mengikut tahap risiko yang telah digariskan secara spesifik.

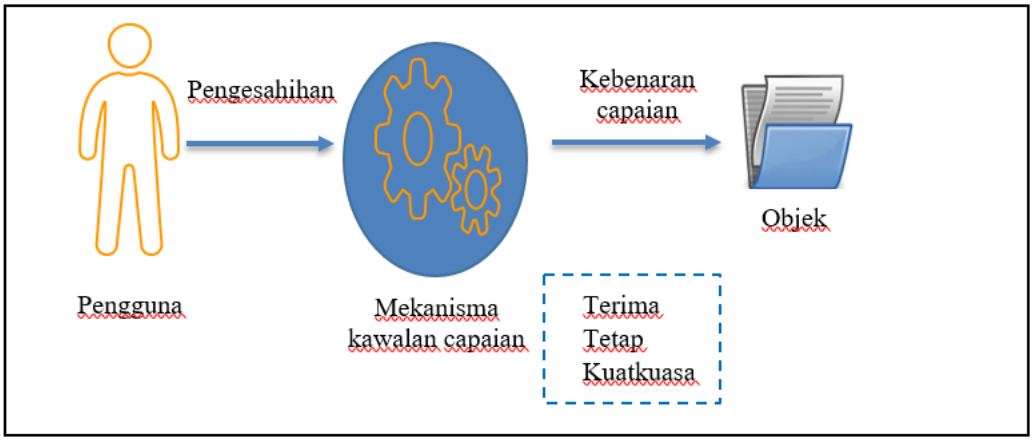
Selain itu, kawalan capaian berasaskan risiko menghubungkan fungsi metrik risiko dengan setiap permintaan capaian dalam membenarkan atau menafikan akses pengguna. Bukan itu sahaja, model kawalan capaian berasaskan risiko berupaya mengendalikan permintaan capaian yang tertentu secara fleksibel dalam proses capaian maklumat dan sumber. Namun, terdapat keperluan untuk mengembangkan potensi model RAdAC sedia ada selaras dengan evolusi pembangunan kawalan capaian yang terfokus ke arah penambahbaikan kekurangan model yang terdahulu. Kajian lepas dalam pembangunan model RAdAC hanya memfokus kepada pengesahihan akses serta perlindungan sumber namun mengabaikan keperluan memelihara privasi pengguna.

Oleh sebab itu, penyelidikan ini mencadangkan penggunaan token identiti dalam model kawalan capaian berasaskan risiko yang melibatkan identiti samaran pengguna serta interaksi pertukaran maklumat tanpa sedar melalui aplikasi polisi kawalan terlindung. Secara amnya, konsep polisi kawalan terlindung telah berjaya diaplikasikan oleh Li et al. (2016) dalam penyelidikan *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) yang telah dijalankan. Polisi kawalan terlindung bertindak mengurangkan beban tugas pentadbir dengan keupayaannya dalam membahagikan sebahagian besar tanggungjawab pentadbir sistem kepada pengurusan awan sekaligus meminimumkan risiko pendedahan maklumat dan identiti pengguna untuk dimanipulasi oleh pentadbir. Namun, integrasi polisi kawalan terlindung dalam pembangunan model kawalan capaian berasaskan risiko masih belum dikaji secara menyeluruh.

Justeru, pembangunan kerangka kawalan capaian berasaskan risiko dengan polisi kawalan terlindung (RiHAP) di awan ini diharap dapat memudahkan pengguna mengendalikan data masing-masing dalam persekitaran yang dinamik dan fleksibel. Di samping itu, struktur capaian dan entiti identiti pengguna yang disimpan di dalam awan juga dapat dilindungi sekaligus mencakupi aspek perlindungan identiti yang berkesan.

1.2 LATAR BELAKANG

Pemilik objek mempunyai autoriti untuk menguatkuasakan mekanisma kawalan capaian bagi melindungi objek daripada akses yang tidak dibenarkan sekaligus melibatkan pengesahihan identiti pengguna. Prinsip asas kawalan capaian adalah untuk melindungi objek daripada operasi yang tidak dibenarkan dengan aplikasi sistem perlindungan selapis seperti Rajah 1.1. Operasi yang terlibat adalah seperti membuka, memadam dan membaca objek yang dimiliki oleh individu ataupun organisasi.



Rajah 1.1 Prinsip asas kawalan capaian

Kawalan capaian berasaskan risiko telah diperkenalkan untuk mengatasi kekurangan model kawalan capaian yang konvensional seperti *Identification Based Access Control* (IBAC) yang hanya menangani kawalan akses yang statik, tegar dan sokongan yang terhad (Karp et al. 2010). Lazimnya, IBAC menggunapakai mekanisma *Access Control List* (ACL) yang tidak fleksibel di mana pengesahihan akses pengguna dilakukan dengan merujuk dan mengemaskini senarai log pengguna berdaftar yang statik beserta akses pengguna yang dibenarkan sahaja. Selain itu, sokongan terhad IBAC menyukarkan penyelarasan pengesahan pengguna jarak jauh serta menyulitkan proses pengurusan pentadbiran pengguna apabila had maksimum kapasiti pengguna berdaftar telah dicapai (Boyko et al. 2000). Justeru, kawalan capaian yang konvensional tidak dapat menampung peningkatan jumlah pengguna berdaftar yang mendadak sekaligus menyukarkan pentadbir sistem untuk mengendalikan log daftar pengguna setiap kali berlaku perubahan akses atau pengemaskinian maklumat pengguna yang terbaharu.

Dalam usaha untuk mengatasi kekurangan model IBAC, Sahai & Waters (2005) telah memperkenalkan konsep *Attribute Based Encryption* (ABE) yang berupaya menangani masalah pengendalian ACL dalam persekitaran pengkomputeran awan yang dinamik. ABE menggunapakai konsep penyulitan maklumat yang tidak terhad kepada kawalan akses yang statik sahaja dengan memastikan akses pengguna sepadan dengan atribut telah ditetapkan. Sebagai contoh, ketua jabatan hanya membenarkan pengguna X yang menepati atribut {"ketua bahagian", "kewangan", "kelulusan"} sahaja untuk menyahsulit akses kepada sesuatu dokumen kewangan.

Walaupun penggunaan konsep IBAC and ABE masih digunapakai secara meluas, kawalan capaian berasakan risiko dilihat berupaya menjadi model kawalan capaian evolusi terkini kerana tidak banyak penyelidikan kawalan capaian yang menjurus kepada pengurusan risiko dijalankan (Fall et al. 2016). Kawalan capaian berasaskan risiko menerapkan konsep menganalisa permintaan capaian secara dinamik di mana akses capaian hanya akan dibenarkan secara bersyarat berpandukan metrik risiko yang telah ditetapkan. Penilaian risiko dijadikan sebagai faktor input yang menentukan samada akses capaian dibenarkan ataupun tidak (Fall et al. 2016; Ricardo dos Santos et al. 2016).

Justeru, kawalan capaian berasaskan risiko merupakan model kawalan capaian yang dicadangkan dalam penyelidikan ini dengan integrasi bersama polisi kawalan terlindung. Kajian terdahulu membuktikan bahawa polisi kawalan terlindung telah berjaya diaplikasikan dalam model kawalan capaian CP-ABE yang diperkenalkan oleh Li et al. (2016). Cadangan pembangunan kerangka kawalan capaian berasaskan risiko dengan polisi kawalan terlindung (RiHAP) diharap dapat mengoptimumkan keberkesanan perlindungan identiti dan keselamatan sistem apabila kebolehupayaan model kawalan capaian ditingkatkan dengan cadangan penambahbaikan fungsi sedia ada.

1.3 PERNYATAAN MASALAH

Peningkatan mendadak terhadap keperluan kawalan capaian dalam pengkomputeran awan telah membangunkan kompetensi pakar keselamatan komputer dalam merekabentuk mekanisma keselamatan yang berupaya berfungsi secara menyeluruh.

Dalam masa yang sama, cabaran dalam menangani risiko keselamatan dalam persekitaran awan masih berada di tahap yang tinggi (Hepsiba & J.G.R.Sathiaseelan 2016; Y. Liu et al. 2015) dalam usaha untuk menyediakan platform keselamatan awan yang berkesan. Justeru, keperluan keselamatan dalam sistem berasaskan awan perlu dikaji untuk mengatasi jurang keselamatan dalam melaksanakan stategi dan justifikasi ke arah membentuk kawalan capaian yang berkesan.

Justeru, pelbagai kajian telah dijalankan untuk mengembangkan potensi model kawalan capaian sedia ada. Fall et al. (2016) telah mengoptimumkan fungsi dan kebolehupayaan model dengan cadangan aplikasi algorithma pengesahan yang fleksibel dalam sistem kawalan capaian untuk memenuhi keperluan persekitaran awan yang bersifat dinamik. Dalam masa yang sama, fungsi statik model kawalan capaian sedia ada telah berjaya dipertingkat dengan penambahan aspek pengesahan selaras dengan keperluan menawarkan teknologi terkini dalam menangani aspek fleksibiti dan dinamik.

Selain itu, terdapat kekurangan dalam aspek kawalan privasi apabila masih terdapat keraguan di pihak pengguna untuk memastikan agar data peribadi yang disimpan adalah selamat tanpa risiko pendedahan maklumat kepada pihak ketiga (Che et al. 2011). Justeru, terdapat keperluan dalam meminimumkan risiko kebocoran maklumat dengan memastikan model kawalan capaian mampu bertindak sebagai medium perantaraan berpusat dalam menguruskan transaksi maklumat yang selamat sekaligus berupaya bertindak mengikut keperluan pengguna. Walau bagaimanapun, fokus utama kawalan capaian berasaskan risiko hanya tertumpu kepada penyulitan data storan di awan serta mengabaikan keperluan untuk melindungi identiti pengguna apabila capaian akses dibenarkan. Kebarangkalian identiti pengguna terdedah semasa proses penyulitan dan penyahsulitan adalah sangat tinggi. Justeru, kekurangan ini membuka ruang kepada implementasi polisi kawalan terlindung dengan aplikasi Protokol *Oblivious Commitment Based Envelope* (OCBE) yang berupaya menjamin kerahsiaan data dan privasi pengguna semasa proses transaksi maklumat berlaku.

Kesimpulannya, ketiadaan aspek perlindungan identiti pengguna dilihat gagal menyediakan persekitaran awan dengan kawalan capaian yang komprehensif. Dalam

masa yang sama, keperluan kepada perlindungan sumber secara menyeluruh masih dikekalkan sebagai titik fokus dalam meningkatkan keselamatan hab storan digital. Keupayaan model kawalan capaian berasaskan risiko dalam menawarkan perlindungan sumber secara menyeluruh masih menjadi tanda tanya sekiranya aspek perlindungan identiti pengguna tidak diambil kira sebagai salah satu daripada keperluan kajian.

1.4 OBJEKTIF KAJIAN

Cadangan pembangunan entiti dan komponen kerangka RiHAP perlu memenuhi keperluan keselamatan awan yang telah dikenalpasti dalam memastikan identiti pengguna dilindungi. Kajian ini adalah berpandukan kepada tiga objektif utama seperti berikut:

1. Mengenalpasti keperluan keselamatan dalam pengkomputeran awan bagi pelaksanaan sistem kawalan capaian yang berkesan daripada aspek perlindungan identiti pengguna.
2. Mencadangkan kerangka kawalan capaian berasaskan risiko dengan polisi kawalan terlindung (RiHAP) dalam storan awan.
3. Mencadangkan instrumen pengesahan ke atas kebolehlaksanaan dan kesesuaian kerangka RiHAP untuk penilaian pakar.

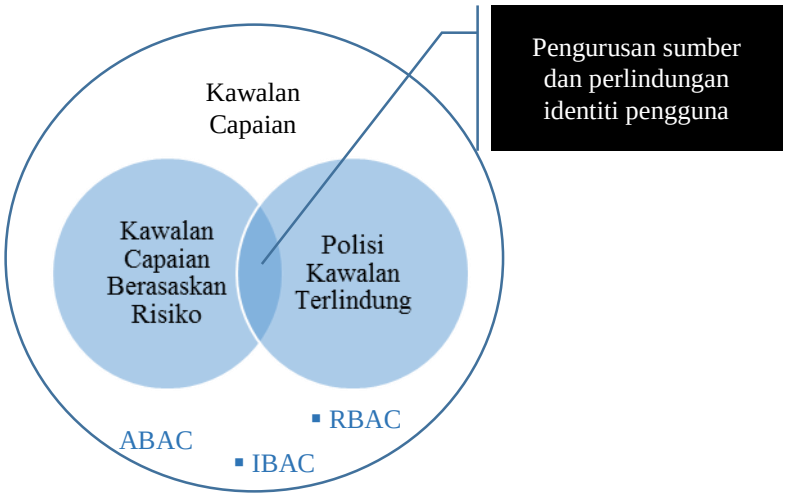
1.5 SOALAN KAJIAN

Kajian ini adalah berpandukan kepada soalan kajian seperti di bawah:

1. Apakah keperluan keselamatan dalam pengkomputeran awan yang mempengaruhi pelaksanaan sistem kawalan capaian yang berkesan?
2. Bagaimanakah keperluan keselamatan awan yang dikenalpasti dapat membangunkan kerangka kawalan capaian berasaskan risiko dengan polisi kawalan terlindung (RiHAP) dalam pengkomputeran awan?
3. Bagaimanakah pelaksanaan cadangan kerangka RiHAP dapat dinilai dan disahkan?

1.6 SKOP KAJIAN

Kajian ini adalah tertumpu kepada penambaikan keupayaan model kawalan capaian berasaskan risiko dengan perlindungan identiti pengguna dan pengurusan sumber yang berkesan seperti Rajah 1.2. Skop utama kajian ini adalah perlindungan maklumat identiti pengguna dengan implementasi protokol OCBE. Selain itu, kajian ini juga mencadangkan pengurusan sumber yang berkesan dengan aplikasi skema pengesahihan akses pengguna di awan yang menggunakan kata laluan dan token identiti sebelum penilaian risiko berlaku. Justeru, pengurusan sumber dan perlindungan identiti pengguna merupakan fokus utama dalam kajian ini untuk membentuk kerangka RiHAP dalam pengkomputeran awan.

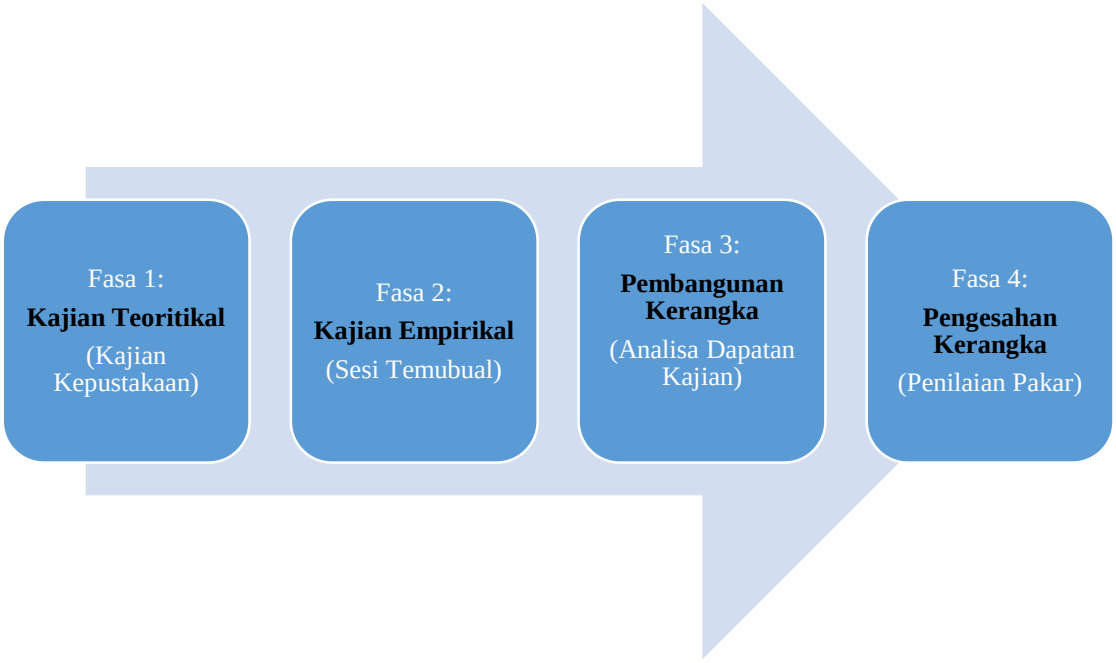


Rajah 1.2 Skop Kajian

1.7 KAEDAH KAJIAN

Terdapat empat fasa yang terlibat dalam penyelidikan ini seperti yang ditunjukkan dalam Rajah 1.3. Kajian teoritikal merupakan fasa pertama yang bermula dengan analisa kajian kepustakaan yang terfokus kepada tajuk kajian lepas sedia ada yang berkaitan dengan penyelidikan ini. Seterusnya, kajian empirikal di fasa kedua melibatkan proses pengumpulan data serta analisa dokumen yang berkaitan dengan pelaksanaan kaedah temubual bersama perunding dan pegawai yang berkecimpung dalam pengurusan teknologi awan. Pada fasa ketiga, pembangunan kerangka telah dicadangkan berdasarkan hasil dapatan daripada kajian teoritikal dan kajian empirikal

yang telah dilaksanakan. Fasa keempat pula menjurus kepada proses pengesahan kerangka yang melibatkan penilaian pakar. Perkara ini akan dibincangkan dengan lebih lanjut dalam 3Bab III metodologi kajian.



Rajah 1.3 Fasa Kajian

1.8 KEPENTINGAN KAJIAN

Pembangunan model kawalan capaian berasaskan risiko merupakan evolusi terkini dalam pembangunan model kawalan capaian yang cenderung ke arah penawaran fungsi yang lebih fleksibel. Pemilihan model kawalan capaian berasaskan risiko dilihat mampu memenuhi keperluan semasa dalam keselamatan maklumat serta berupaya menyokong persekitaran pengkomputeran awan yang dinamik dengan lebih berkesan (Ricardo dos Santos et al. 2016).

Justeru, cadangan integrasi polisi kawalan terlindung dalam pembangunan model kawalan capaian berasaskan risiko diharap mampu memberikan impak dan

sumbangan dalam dunia penyelidikan model kawalan capaian masa kini. Sistem Perlindungan Dua Lapis dengan janaan token identiti berupaya membentuk modul keselamatan yang bersepadu dalam infrastruktur awan. Cadangan pembangunan kerangka RiHAP dengan Sistem Perlindungan Dua Lapis menyediakan platform keselamatan yang kukuh sekaligus meningkatkan kebolehpercayaan dan kebolehsuaian sistem.

1.9 ORGANISASI DISERTASI

Pengurusan disertasi ini disediakan mengikut bab berdasarkan keperluan kajian. Bab I membincangkan secara umum tentang pengenalan dan latar belakang kajian. Berdasarkan pernyataan masalah yang dinyatakan, objektif dan soalan kajian dirangka untuk mencapai matlamat kajian. Seterusnya, skop kajian ditentukan dan kaedah kajian dirangka berdasarkan empat fasa yang telah ditetapkan. Bab ini juga mengandungi kepentingan kajian, organisasi disertasi dan disimpulkan melalui rumusan.

Bab II merupakan sorotan kajian kepustakaan secara menyeluruh ke atas kajian lampau yang berkaitan dengan pengkomputeran awan, kawalan capaian, kawalan capaian berasaskan risiko, analisa kerangka kawalan capaian berasaskan risiko, polisi kawalan terlindung dan prinsip umum pengesahihan. Kajian teoritikal dijalankan untuk mengenalpasti kekurangan dan kelebihan bagi setiap aspek yang dibincangkan seterusnya merangka cadangan pembangunan kerangka konsep RiHAP.

Seterusnya, Bab III membincangkan tentang pendekatan kajian kualitatif yang diaplikasikan sepanjang penyelidikan ini. Setiap aktiviti kajian dihuraikan mengikut empat fasa yang terlibat iaitu kajian teoritikal, kajian empirikal, pembangunan kerangka dan pengesahan kerangka. Di samping itu, teknik analisa kandungan yang dilaksanakan dalam kajian kualitatif ini dihuraikan secara lebih spesifik.

Bab IV pula merangkumi analisa dan interpretasi data berdasarkan dapatan kajian kualitatif yang dijalankan serta keperluan keselamatan yang telah dibincangkan. Seterusnya, cadangan pembangunan kerangka RiHAP dirumuskan berdasarkan skema pengesahihan akses dan analisa keselamatan tidak formal yang dijalankan.

Selain itu, Bab V mengandungi dapatan kajian berdasarkan pengesahan pakar yang merangkumi analisis dan rumusan penilaian pakar. Seterusnya, pembangunan kerangka RiHAP juga akan diperincikan mengikut fungsi dan aliran kerja yang spesifik.

Bab VI merupakan rumusan dan penutup yang membincangkan tentang pencapaian objektif kajian, sumbangan kajian, batasan kajian dan cadangan kajian pada masa hadapan.

1.10 RUMUSAN

Pengkomputeran awan merupakan platform terbaik masa kini dalam memenuhi peningkatan kehendak pengguna terhadap keupayaan storan, keperluan keselamatan komputer yang tinggi serta persekitaran yang dinamik. Justeru, model kawalan capaian berasaskan risiko dilihat berupaya menjadi medium yang fleksibel dalam usaha untuk menyediakan kawalan keselamatan yang optimum dalam pengkomputeran awan. Selain itu, implementasi polisi kawalan terlindung dalam model RAdAC pula menjamin perlindungan identiti pengguna sekaligus melindungi sumber daripada ancaman. Kesimpulannya, penyelidikan ini mencadangkan pembangunan kerangka RiHAP dalam pengkomputeran awan dengan penawaran fungsi perlindungan identiti pengguna.

BAB II

KAJIAN KEPUSTAKAAN

2.1 PENGENALAN

Teknologi awan dilihat sebagai revolusi terkini dalam dunia teknologi maklumat yang menawarkan kelebihan dalam mengendalikan storan maya secara lebih fleksibel melalui pelaksanaan kawalan capaian yang berkesan. Bukan itu sahaja, teknologi awan yang dilengkapi dengan tahap kerentanan yang tinggi melalui pelaksanaan polisi kawalan terlindung dapat menyediakan persekitaran awan yang berupaya menangani cabaran keselamatan dan privasi.

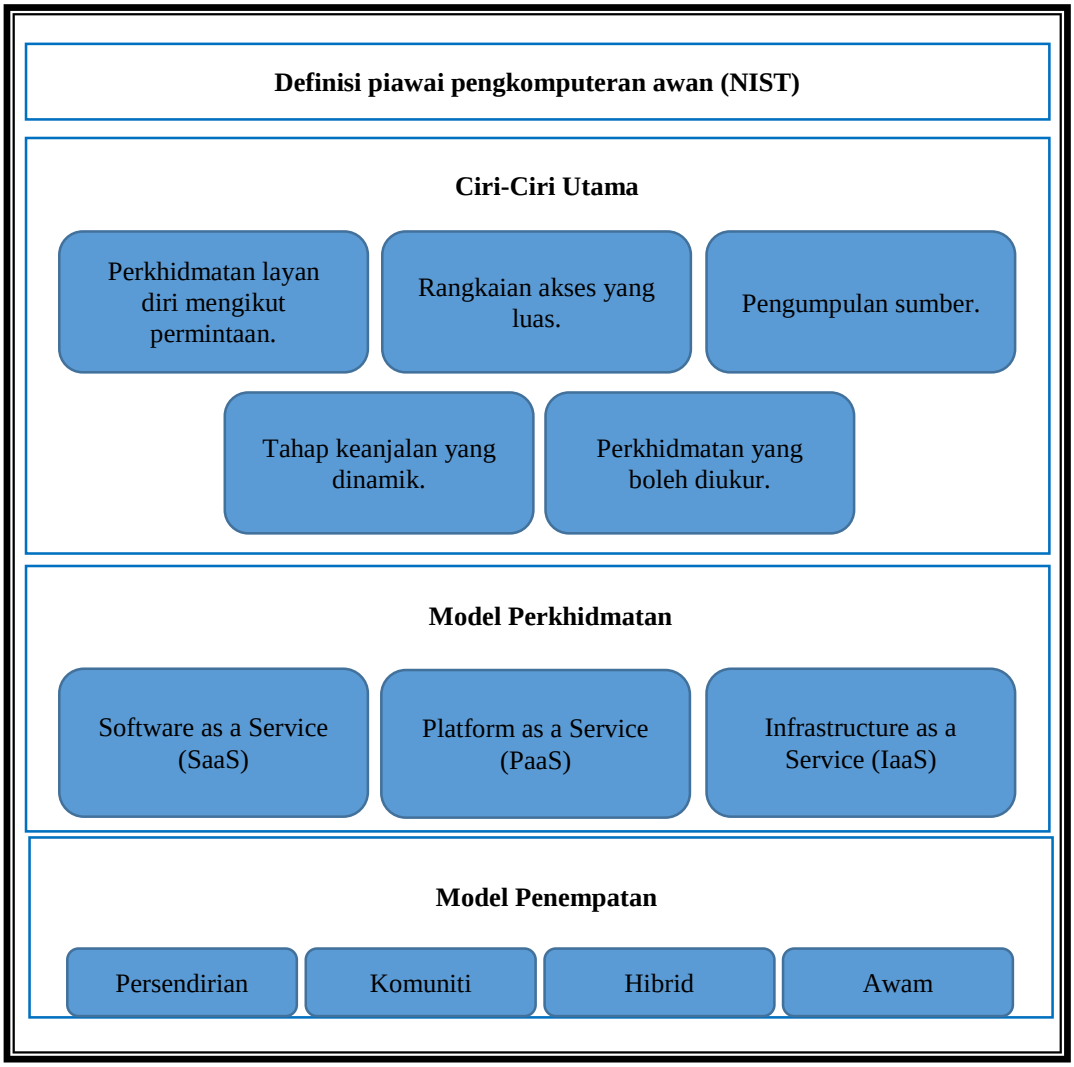
Bab ini akan membincangkan secara lebih terperinci mengenai pengkomputeran awan dari aspek definisi, konsep, cabaran awan sekaligus merumuskan mengenai keperluan keselamatan yang perlu dititikberatkan dalam persekitaran awan yang kondusif. Seterusnya, bab ini akan menjelaskan dengan lebih lanjut berkenaan kawalan capaian, kawalan capaian berasaskan risiko dan polisi kawalan terlindung yang digunakan sebagai asas dalam membangunkan model kajian. Di akhir bab, kupasan menyeluruh yang dijalankan melalui kajian kepustakaan ini akan dijadikan asas dalam membentuk kerangka RiHAP dalam pengkomputeran awan.

2.2 PENGKOMPUTERAN AWAN

2.2.1 Definisi dan Konsep

Pengkomputeran awan adalah teknologi berteraskan internet yang meliputi perkhidmatan storan dan komunikasi, pengurusan sumber yang efisien serta kos yang minima. Merujuk kepada piawaian definisi yang ditetapkan oleh *National Institute of Standards and Technology (NIST)*, pengkomputeran awan adalah model yang

membenarkan akses rangkaian mengikut permintaan kepada sumber pengkomputeran terkonfigurasi (rangkaian, pelayan, storan, aplikasi dan perkhidmatan) untuk kegunaan pantas dengan pengurusan pentadbiran yang minima atau interaksi penyedia perkhidmatan (Mell & Grance 2011).



Rajah 2.1 Elemen Asas dalam Model Pengkomputeran Awan.

Sumber:Adaptasi daripada Hepsiba & J.G.R.Sathiaseelan 2016; Mell & Grance 2011; Subashini & Kavitha 2011

Rajah 2.1 di atas merupakan model pengkomputeran awan yang melibatkan empat lapisan berbeza yang terdiri daripada definisi, ciri-ciri utama, model perkhidmatan dan model penempatan (Mell & Grance 2011; Subashini & Kavitha 2011). Definisi awan merujuk kepada lapisan pertama yang mencorakkan lima ciri-ciri utama pengkomputeran awan di lapisan kedua sekaligus memacu penglibatan pengguna dalam model perkhidmatan dan model penempatan awan.

Perkhidmatan layan diri mengikut permintaan merupakan keupayaan pengguna untuk mengendalikan fungsi pengkomputeran tanpa interaksi dengan penyedia perkhidmatan. *Rangkaian akses yang luas* ialah kebolehcapaian rangkaian daripada platform pengguna yang berbeza. Selain itu, *pengumpulan sumber* seperti storan dan jalur lebar rangkaian diuruskan secara setempat oleh penyedia perkhidmatan mengikut permintaan daripada pengguna yang berbeza. *Tahap keanjalan yang dinamik* merupakan keupayaan pengurusan sumber dan pengguna secara berskala pada bila-bila masa. *Perkhidmatan yang boleh diukur* pula adalah keupayaan awan untuk mengawal dan menggunakan sumber secara optimum dengan elemen pengukuran secara automatik.

Lapisan ketiga yang merangkumi *Software as a Service (SaaS), Platform as a Service (PaaS)* dan *Infrastructure as a Service (IaaS)* adalah tiga model perkhidmatan dalam pengkomputeran awan (Hari Krishna et al. 2016). Penyedia perkhidmatan menyediakan perisian aplikasi mengikut permintaan pengguna dalam *SaaS*. *PaaS* pula membenarkan persekitaran pengaturcaraan yang disokong oleh penyedia perkhidmatan manakala penyedia perkhidmatan menyediakan komponen infrastruktur secara maya kepada pengguna dalam *IaaS*.

Selain itu, lapisan keempat mengandungi empat model penempatan iaitu persendirian, awam, hibrid dan komuniti (Hepsiba & J.G.R.Sathiaseelan 2016; Mell & Grance 2011; Subashini & Kavitha 2011). Awan persendirian merupakan persekitaran yang dibangunkan secara dalaman dengan sumber-sumber yang khusus untuk organisasi yang tertentu manakala awan awam merupakan persekitaran yang dibangunkan untuk kegunaan umum. Selain itu, awan komuniti disasarkan untuk kumpulan pelanggan tertentu yang berkongsi kepentingan yang sama manakala awan hibrid adalah gabungan dua atau lebih awan (persendirian, awam atau komuniti).

Kefahaman pengguna berkenaan model pengkomputeran awan dan kepentingannya, serta penggunaan awan secara berhemah telah meningkatkan potensi awan untuk berkembang dalam industri teknologi maklumat. Memandangkan jumlah dokumentasi yang dihasilkan semakin meningkat dari sehari ke sehari, pengguna mula beralih kepada teknologi yang mampu menyediakan storan yang berupaya menampung

keperluan pengguna dan persekitaran yang dinamik. Walaupun pengkomputeran awan mampu melindungi aset dan identiti pengguna, namun tahap keraguan pengguna berkenaan kawalan keselamatan, privasi dan kebolehpercayaan masih tinggi.

Kegagalan melengkapkan pengkomputeran awan dengan kawalan keselamatan yang tinggi akan membuka ruang kepada capaian berniat jahat oleh pengguna hasad sekaligus menjurus kepada masalah kebocoran maklumat. Tahap privasi di persekitaran awan membantu memelihara kerahsiaan data dan melindungi identiti pengguna manakala tahap kebolehpercayaan pula melibatkan pengurusan awan yang berkesan dalam menyediakan perkhidmatan storan dan komunikasi yang menepati kehendak pengguna. Justeru, perkembangan teknologi awan di organisasi adalah bergantung kepada tahap privasi dan kebolehpercayaan yang ditawarkan oleh pengkomputeran awan.

Situasi ini telah mendorong pengkaji untuk menjalankan penyelidikan yang berfokus kepada cabaran dalam mengendalikan teknologi awan. Suzic et al. (2015) telah menerangkan dengan lebih lanjut tentang usaha dan inisiatif organisasi untuk membangunkan program seperti FT7, SWIFT dan POSITIF bagi mengkaji dan menambahbaik dimensi senibina awan pada masa hadapan. Antara inisiatif yang telah dijalankan adalah mengkaji awan daripada aspek pengurusan keselamatan, cabaran privasi, pengurusan identiti dan pendekatan keselamatan awan daripada perspektif pengurusan atasan.

Subashini & Kavitha (2011) telah menghuraikan berkenaan cabaran yang boleh mendatangkan ancaman kepada pengkomputeran awan serta langkah-langkah keselamatan bagi menangani masalah tersebut. Namun, kajian tersebut hanya tertumpu kepada isu-isu dan langkah-langkah keselamatan semasa tanpa mengulas mengenai perspektif awan untuk jangka masa panjang. Walau bagaimanapun, analisa kekuatan dan kelemahan yang dijalankan oleh Liu et al. (2015) terhadap penyelesaian masalah keselamatan telah menghasilkan jangkaan hala tuju penyelidikan awan pada masa hadapan untuk mengekalkan persekitaran awan yang selamat. Selain itu, kajian yang dijalankan oleh Hepsiba & J.G.R.Sathiaseelan (2016) pula terfokus ke arah cabaran bagi

model perkhidmatan awan namun penyelesaian masalah keselamatan yang dicadangkan lebih tertumpu kepada *Cloud Service Provider* (CSP) sahaja.

Masalah kebolehpercayaan juga merupakan salah satu aspek penting dalam menyokong sistem pembuat keputusan sekaligus meyakinkan pengguna bahawa sistem yang digunakan ataupun sumber yang diperolehi adalah selamat dan tepat (Zissis & Lekkas 2012). Antara proses yang terlibat dalam mengatasi masalah kebolehpercayaan adalah kaedah pengenalpastian dan pengesahihan pengguna bagi menjamin keselamatan sistem yang ditempatkan di awan daripada ancaman dan serangan luaran dan dalaman. Justeru, penilaian keselamatan awan berpandukan perspektif keselamatan adalah diperlukan dalam menghasilkan cadangan penyelesaian yang berdaya maju untuk menangani ancaman keselamatan awan.

Kesimpulannya, proses mengenalpasti isu dan risiko keselamatan dalam mengendalikan teknologi awan di organisasi merupakan aspek penting bagi meningkatkan tahap kecenderungan pengguna dalam memanfaatkan kelebihan teknologi tersebut. Bahagian seterusnya akan membincangkan tentang pengendalian ciri-ciri utama pengkomputeran awan untuk mengenalpasti tahap keupayaan dan keperluan keselamatan awan dalam mengendalikan kawalan capaian yang berkesan.

2.2.2 Keperluan Keselamatan dalam Pengkomputeran Awan.

Perkembangan teknologi awan bergantung kepada jaminan keselamatan dan tahap privasi yang tinggi. Kajian yang dijalankan oleh pengkaji terdahulu terhadap cabaran dalam pengkomputeran awan merupakan pemangkin dan peneraju dalam menyediakan persekitaran awan yang komprehensif. Kajian yang dijalankan oleh ISACA/CSA (2015) mendedahkan bahawa keselamatan dan privasi merupakan kebimbangan utama di kalangan responden dengan mencatat peratusan tertinggi sebanyak 54% . Responden yang terlibat adalah terdiri daripada Ketua Pegawai Maklumat (CIO) dan pegawai yang terlibat dalam pengurusan teknologi untuk membantu kajian dalam mengenalpasti keperluan dan kepentingan teknologi awan kepada organisasi (ISACA/CSA 2015). Di samping itu, Jadual 2.1 merupakan ringkasan penyelidikan yang telah dijalankan oleh penyelidik terdahulu dalam menangani cabaran mengendalikan perkomputeran awan.

Jadual 2.1 Cabaran dan Cadangan Penyelesaian dalam Pengkomputeran Awan

Sumber	Cabaran	Cadangan Penyelesaian
Takabi et al. (2010)	▪ Pengesahihan dan pengurusan identiti. ▪ Ketidakberkesanan kawalan capaian. ▪ Kebolehpercayaan. ▪ Privasi dan kebocoran data.	▪ Pengurusan identiti yang berpusat. ▪ Model kawalan capaian yang berkesan. ▪ Membangunkan kerangka keselamatan. ▪ Penyulitan kriptografi.
Che et al. (2011)	▪ Pencerobohan dan serangan luar. ▪ Pengurusan identiti dan pengesahihan akses capaian.	▪ Pengurusan keselamatan yang berkesan. ▪ Kawalan capaian yang berkesan.
Subashini & Kavitha (2011)	▪ Keselamatan, integriti, kerahsiaan dan capaian data. ▪ Persekitaran maya yang terdedah kepada ancaman. ▪ Ketersediaan, pengurusan identiti dan pengesahihan capaian.	▪ Membangunkan piawaian keselamatan awan. ▪ Membangunkan kerangka keselamatan awan yang berkesan. ▪ Penyulitan dan kawalan capaian.
Zissis & Lekkas (2012)	▪ Kerahsiaan dan privasi. ▪ Integriti. ▪ Ketersediaan.	▪ Menerapkan piawai keselamatan. ▪ Kerangka keselamatan yang sah. ▪ Kriptografi untuk penyulitan. ▪ Kawalan capaian yang berkesan.
Shahzad (2014)	▪ Nafi khidmat (DoS) ▪ Keselamatan storan awan ▪ Integriti, kerahsiaan dan ketersediaan data.	▪ Kawalan capaian yang berkesan. ▪ Pengurusan identiti yang berkesan. ▪ Penyulitan untuk pengesahihan akses.
Y. Liu et al. (2015)	▪ Ketidakberkesanan kawalan data. ▪ Pengendalian storan maya. ▪ Pengesahihan identiti dalam persekitaran maya. ▪ Lemah pengurusan keselamatan	▪ Penyulitan. ▪ Perkukuh kawalan capaian. ▪ Pengurusan keselamatan yang efektif.
Suzic et al. (2015)	▪ Pengurusan identiti. ▪ Pengesahihan capaian dan kebolehpercayaan.	▪ Model kawalan capaian. ▪ Mekanisma kriptografi untuk penyulitan.
Hepsiba & J.G.R.Sathiaseelan (2016)	▪ Pencerobohan dan serangan dari dalam/ ancaman luar. ▪ Nafi khidmat (DoS) ▪ Keselamatan, integriti, kerahsiaan dan ketersediaan data.	▪ Prosedur penyulitan yang kukuh dan kawalan capaian. ▪ Menambahbaik pengurusan keselamatan maklumat. ▪ Protokol pengesahihan yang fleksibel dan berkesan.

Jadual di atas merumuskan penyelidikan yang telah dijalankan oleh pengkaji terdahulu dalam mengenalpasti cabaran dan merumuskan cadangan penyelesaian dalam mengendalikan persekitaran awan (Hepsiba & J.G.R.Sathiaseelan 2016; Y. Liu et al. 2015; Subashini & Kavitha 2011; Suzic et al. 2015). Justeru, pengurusan keselamatan dalam pengendalian awan perlu mengambilkira pelbagai keperluan keselamatan dalam sistem berasaskan awan seperti berikut:

a) Kebolehpercayaan.
   Menyokong sistem pembuat keputusan dalam meyakinkan pengguna bahawa sumber yang dilindungi itu adalah betul dan selamat.

b) Keselamatan data.
   Melindungi data daripada ketirisan maklumat akibat daripada serangan luaran ataupun ancaman dalaman.

c) Integriti data.
   Perlindungan data daripada penggubahan maklumat melalui pengemaskinian, pengubahsuaian, pemalsuan data.

d) Capaian data.
   Capaian data merujuk kepada penguatkuasaan polisi keselamatan untuk menjamin kebenaran capaian di kalangan pengguna yang sah sahaja.

e) Kerahsiaan.
   Kerahsiaan merujuk kepada kebenaran akses yang hanya diberikan kepada pengguna ataupun subjek yang dibenarkan untuk capaian kepada objek ataupun data yang dilindungi.

f) Pengesahihan pengguna.
   Proses mengenalpasti entiti yang sah semasa transaksi ataupun peralihan maklumat mengikut kelayakan pengguna (peranan, kebenaran akses dan sebagainya).

g) Ketersediaan sistem.

Ketersediaan merujuk kepada kebolehan sistem yang merangkumi data, perisian dan perkakasan untuk beroperasi mengikut permintaan pengguna.

h) Pengurusan identiti pengguna.

Pengurusan identiti yang melibatkan tindakan mewujudkan dan menyekat akses kelayakan pengguna berdasarkan ID pengguna ataupun/serta pengesahan sijil digital/ token/ kad pintar pengguna yang mewakili identiti pengguna.

Keperluan keselamatan yang digariskan seperti di atas juga memenuhi keperluan Prinsip Keselamatan Maklumat iaitu ketersediaan (*availability*), integriti (*integrity*) dan kerahsiaan (*confidentiality*) (Hari Krishna et al. 2016). Namun, cabaran terbesar dalam memastikan Prinsip Keselamatan Maklumat terjamin adalah memastikan awan berupaya memproses sumber tanpa mempunyai pengetahuan atau maklumat mengenai sumber tersebut (Ryan 2013). Perkara ini akan dikupas dengan lebih lanjut dalam bahagian 2.6.2.6 below

Kesimpulannya, keperluan keselamatan yang telah dikenalpasti merupakan penanda aras ke arah melestarikan persekitaran awan dengan kawalan keselamatan sumber dan perlindungan identiti pengguna yang lebih terjamin. Selain itu, pembangunan komponen dan entiti tertentu dalam kerangka RiHAP yang dicadangkan perlu memenuhi keperluan keselamatan yang telah digariskan. Dalam masa yang sama, penyedia perkhidmatan awan yang mampu menawarkan tahap keselamatan dan kebolehpercayaan yang tinggi berupaya menjadi pilihan pengguna sebagai peneraju perkhidmatan (ISACA/CSA 2015).

Kajian yang dijalankan oleh ISACA/CSA (2015) merumuskan bahawa potensi pengguna baharu untuk beralih ke arah teknologi pengkomputeran awan dapat ditingkatkan apabila masalah keselamatan dan privasi berjaya ditangani dengan lebih berkesan. Justeru, strategi baharu dalam meningkatkan keupayaan model RAdAC sedia ada perlu dirangka dengan kapasiti baharu yang berfungsi dalam melindungi identiti pengguna dan keselamatan hab storan digital. Bahagian 2.3 dan seterusnya akan mengupas konsep dan kepentingan kawalan capaian secara menyeluruh.

2.3 KAWALAN CAPAIAN

2.3.1 Definisi dan Konsep

Aspek keselamatan dan privasi adalah unsur penting dalam meningkatkan tahap kebolehpercayaan awan. Justeru, sistem storan di awan perlu dilengkapkan dengan kawalan capaian yang berupaya memenuhi keperluan asas keselamatan dalam membenarkan, menafikan dan mengehadkan akses kepada pengguna. Kawalan capaian juga berupaya memantau dan merekod akses pengguna sekaligus mengenalpasti cubaan akses daripada pengguna yang tidak berdaftar bagi melindungi aset penting sesuatu organisasi. Oleh itu, pelbagai model kawalan capaian telah dicadangkan dan dibangunkan oleh pengkaji terdahulu dalam menyediakan persekitaran awan yang selamat dan kondusif.

Evolusi kawalan capaian bermula dengan kesedaran pengguna tentang kepentingan kawalan dokumentasi mengikut pengguna yang berbeza dalam awan yang sama (Karp et al. 2010). Di peringkat awal era pengkomputeran, identiti pengguna merupakan entiti utama yang membenarkan capaian pengguna kepada sesuatu sistem atau dokumentasi. Justeru, keperluan untuk berkongsi maklumat dengan menggunakan identiti pengguna sebagai salah satu keperluan bagi proses kebenaran capaian telah menjadi pemangkin kepada pembangunan model kawalan capaian yang selamat.

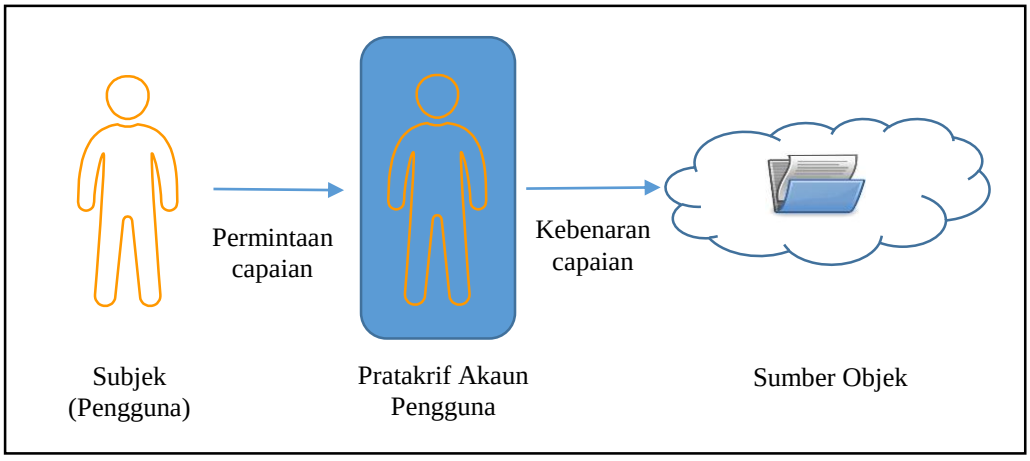
2.3.2 Model Kawalan Capaian

Antara model kawalan capaian yang telah dibangunkan oleh pengkaji terdahulu adalah IBAC, RBAC, ABAC dan RAdAC. Di awal pengenalan model kawalan capaian, IBAC telah dibangunkan dan terfokus kepada pengurusan identiti pengguna dengan menggunapakai kaedah kawalan capaian ACL di mana kebenaran untuk mengakses sumber dokumen bergantung kepada identiti pengguna secara berpusat (Sahai & Waters 2005). Walau bagaimanapun, model IBAC adalah statik dan rigid kerana dasar kebergantungan pengguna kepada pengurus dokumen untuk membuat sebarang perubahan kepada sumber dokumen (Karp et al. 2010). Selain itu, pendekatan kawalan capaian dengan menggunakan IBAC juga berisiko untuk terdedah kepada kecurian

maklumat pengguna dan kata laluan serta kegagalan mengurus sistem teragih secara berkesan (Liao et al. 2006).

Justeru, RBAC telah diperkenalkan untuk mengatasi masalah sistem teragih dan mengurangkan kebergantungan kepada ACL (Karp et al. 2010). RBAC membenarkan akses pengguna mengikut peranan masing-masing sekaligus memudahkan pengemaskinian sistem. Sebagai contoh, pengguna dengan peranan Pengurus dibenarkan untuk mengakses set dokumentasi yang berbeza berbanding pengguna dengan peranan Pengaturcara Komputer. Namun demikian, peranan pengguna yang sentiasa berubah dan kegagalan RBAC dalam menyokong persekitaran yang dinamik merupakan kekangan dalam meneruskan legasi RBAC di pengkomputeran awan.

Rajah 2.2 menggambarkan situasi pengguna yang terlibat dalam persekitaran kawalan capaian secara tradisional seperti IBAC dan RBAC. Akses capaian hanya dibenarkan berdasarkan pratakrif akaun pengguna yang telah ditetapkan lebih awal samada melibatkan senarai identiti pengguna yang telah dikenalpasti (ACL) ataupun peranan pengguna yang telah ditetapkan. Penilaian kebenaran capaian berasaskan identiti dan peranan pengguna dilihat tidak lagi relevan dalam persekitaran awan yang dinamik dan fleksibel. Satu kaedah kawalan capaian yang berkesan perlu dilaksanakan bagi mengelakkan kebergantungan kepada pratakrif identiti ataupun peranan pengguna yang melibatkan pengurusan capaian yang kompleks dan memakan masa.



Rajah 2.2 Kaedah Tradisional Akses Capaian

Sehubungan itu, kajian telah dijalankan bagi menangani kekurangan pelaksanaan kaedah kawalan capaian secara tradisional sehingga kemunculan ABAC (Goyal et al. 2006). Model ini telah menarik perhatian pengguna dalam bidang akademik mahupun industri atas kebolehupayaan ABAC dalam menguatkuasakan polisi kebenaran capaian berdasarkan atribut pengguna dan objek yang sedia ada. Dalam ABAC, akses pengguna hanya akan dibenarkan berdasarkan penilaian atribut subjek (contoh: umur pengguna), objek (contoh: fail), persekitaran (contoh: operasi yang telibat seperti baca dokumen, padam dokumen dan sebagainya) serta penetapan polisi.

Sahai & Waters (2005) telah memperkenalkan konsep *Attribute Based Encryption* (ABE) yang menggunakan konsep ABAC di mana penyulitan maklumat dengan penetapan atribut dilaksanakan untuk mengakses sumber. Sistem ABE menggabungkan kunci pengguna dan *cyphertext* dengan atribut yang telah ditetapkan di mana akses hanya dibenarkan jika atribut dalam kunci pengguna dan *cyphertext* adalah sepadan. Namun, konsep ABE dilihat tidak fleksibel kerana bergantung kepada kesepadanan atribut tanpa mengambilkira faktor perbezaan struktur akses bagi pengguna yang berlainan.

Goyal et al. (2006) pula telah menambahbaik konsep ABE dengan memperkenalkan *Key-Policy* ABE (KP-ABE) di mana kekunci persendirian untuk pengguna yang berlainan mempunyai struktur akses yang berbeza. Walaupun penyelidikan ini telah mengembangkan potensi ABE, namun ia membuka ruang kepada masalah penskalaan dan pembatalan akses pengguna.

Justeru, kajian yang dijalankan oleh Wan et al. (2016) telah memperkenalkan *Hierarchical Attribute-Set-Based Encryption* (HASBE) yang mampu menyokong jumlah pengguna yang berskala besar serta dilengkapkan dengan fungsi pembatalan akses pengguna. Kajian ini mencadangkan fungsi penetapan atribut tarikh luput kepada kunci pengguna sekaligus memudahkan pengemaskinian akses pengguna. Namun, konsep HASBE tidak menyokong sifat awan yang dinamik kerana pengurusan pentadbiran sistem dijangka meningkat untuk menyokong fungsi pengemaskinian tarikh luput.

Sehubungan itu, kajian yang dijalankan oleh Servos & Osborn (2017) membuktikan bahawa walaupun ABAC masih mengalami revolusi dari segi penambahbaikan ataupun pelanjutan rekabentuk model, masih terdapat beberapa masalah yang masih belum diterokai, diabaikan ataupun dicadangkan untuk dikaji pada masa hadapan. Justeru, RAdAC telah diperkenalkan dengan menggunakan konsep ABAC tetapi melibatkan penambahan fungsi konteks maklumat seperti risiko operasi dan kehendak pengguna dalam menentukan keputusan akses (Ricardo dos Santos et al. 2016).

Selain itu, kajian yang dijalankan oleh Choi et al. (2015) telah menggunakan kelebihan model RAdAC dengan menawarkan tindakan pantas dalam menyediakan rawatan perubatan mengikut tahap kondisi pesakit berdasarkan analisa rekod sejarah pesakit sebelum itu. Kajian ini menganggarkan dan menggaplikasikan metrik risiko berdasarkan konteks maklumat pesakit dan profil rawatan terdahulu yang pernah direkodkan dalam sistem untuk menyediakan output rawatan perubatan yang terpercaya.

Jadual 2.2 merumuskan perbandingan variasi model kawalan capaian sedia ada bersama kelebihan dan kekangan masing-masing.

Jadual 2.2 Perbandingan Model Kawalan Capaian Sedia Ada

Sumber: (Karp et al. 2010; Mulimani & Rachh 2016; Ricardo dos Santos et al. 2016)

Kawalan Capaian	**Kelebihan**	**Kekangan**
Identification Based Access Control (IBAC)	Menguruskan pendaftaran identiti dan akses pengguna berdaftar secara berpusat.	▪ Tidak dapat menyokong sistem teragih. ▪ Tidak menyokong peningkatan jumlah pengguna yang drastik. ▪ Pengurusan pentadbiran yang tidak efektif.
Kawalan Capaian Berasaskan Peranan (RBAC)	Menguruskan akses pengguna berdasarkan keistimewaan yang ditetapkan mengikut peranan dan berupaya beroperasi secara tidak berpusat.	▪ Peranan yang sentiasa berubah. ▪ Tidak menyokong peningkatan jumlah pengguna yang drastik dan konteks maklumat. ▪ Kesukaran menetapkan keistimewaan pengguna apabila melibatkan pihak lain.

Bersambung…

…sambungan

Kawalan Capaian	Kelebihan	Kekangan
Kawalan Capaian Berasaskan Atribut (ABAC)	Menguruskan akses pengguna mengikut atribut dan konteks semasa.	▪ Tidak menyokong perubahan atribut pengguna.
Risk Adaptable Access Control (RAdAC)	Menambahbaik pengurusan akses pengguna berpandukan konteks semasa dan penetapan fungsi metrik risiko.	▪ Masih dalam peringkat kajian.

2.4 KAWALAN CAPAIAN BERASASKAN RISIKO.

2.4.1 Pengenalan

Kawalan capaian berasaskan risiko berpotensi besar dalam mengatasi masalah ketika menggunakan skema konvensional ACL bagi pengesahihan kata laluan yang bergantung kepada polisi kawalan akses yang statik dan terdedah kepada kata laluan yang mudah dijangka. Selain itu, pengesahihan kata laluan dalam skema konvensional juga tidak dapat menampung persekitaran yang sentiasa berubah kerana melibatkan peningkatan pengguna dan sumber dalam julat yang lebih besar.

2.4.2 Konsep

Model RAdAC yang diperkenalkan semasa bengkel NIST (*National Institute of Standards and Technology*) pada 2009 telah menggunapakai lima faktor utama yang menentukan keputusan akses iaitu keperluan operasi, risiko keselamatan, faktor situasi, polisi kawalan capaian dan heuristik (Fall et al. 2016).

Keperluan operasi melibatkan hubungan antara pengguna dan sumber yang perlu diakses manakala risiko keselamatan pula melibatkan kebarangkalian antara penentuan risiko dan permintaan. Faktor situasi pula merujuk kepada situasi semasa manakala polisi kawalan capaian melibatkan penguatkuasaan polisi dengan menetapkan paras risiko mengikut kondisi semasa. Selain itu, heuristik melibatkan penggunaan keputusan akses capaian terdahulu dalam menjana keputusan akses yang terkini