BINUS UNIVERSITY ONLINE LEARNING

People
Innovation
Excellence

LECTURE NOTES

MOBI8001 – Mobile Technology & Cloud Computing

Topik 10 - Trust in Mobile Cloud Computing

LEARNING OUTCOMES

1. Peserta mampu menerapkan konsep mobile cloud computing dalam menyelesaikan masalah-masalah teknis di dunia nyata.
2. Peserta memiliki kemampuan dalam menganalisa arsitektur, platform, dan teknologi-teknologi pendukung dari mobile cloud computing.
3. Peserta mampu mengevaluasi kemajuan dan tantangan penelitian dari teknologi mobile cloud computing

OUTLINE MATERI :

1. Introduction
2. Trust Properties
3. Components of Trust
4. Types of Trust
5. Trust Issues
6. Ways of Trust Establishment
7. Trust Evaluation
8. Detailed Study of Various Aspects of Trust in MCC
9. Conclusion

ISI MATERI

1. Introduction

Trust dapat diartikan sebagai keyakinan yang kuat akan kualitas seseorang atau sesuatu seperti dapat diandalkan, kebaikannya, kejujurannya, efektifitas, loyalitas, maupun kemampuannya. Kita cenderung memiliki keyakinan yang kuat pada suatu sistem ketika kita mengetahui sistem tersebut secara lengkap dan sistem tersebut mampu bekerja seperti yang kita harapkan. Pada mobile cloud monputing (MCC), trust merupakan suatu parameter yang sangat vital karena penyimpanan dan pemrosesan data pribadi terjadi pada cloud yang dapat terletak pada lokasi yang jauh dari pengguna. Di sisi lain, para provider layanan cloud (CSP) juga harus senantiasa mengevaluasi para penggunanya sehingga dapat mendorong penggunaan cloud oleh pengguna yang dapat dipercaya dan juga mampu menghilangkan pengguna-pengguna jahat dari sistem. Suatu hubungan yang saling percaya di antara para penyedia dan pemakai layanan cloud sangatlah diperlukan untuk mendukung penerapan MCC secara efektif di seluruh dunia.

2. Trust Properties

Ada beberapa property atau sifat-sifat dari trust yang penting untuk diketahui, di antaranya:

- Trust is field specific: Trust memiliki atribut yang berbeda pada bidang aplikasi yang berbeda. Jadi, arti dari trust perlu dibatasi pada suatu atau beberapa bidang tertentu.
- In mathematical sense, trust is not symmetric: Ketika suatu entitas X mempercayai suatu entitas lain Y, belum tentu entitas lain tersebut, Y, juga mempercayai entitas X.
- Trust is not transitive: Ketiga entitas X mempercayai entitas Y, kemudian entitas Y mempercayai entitas Z, hal ini tidak berarti bahwa entitas X juga mempercayai entitas Z.
- Trust may change dynamically: Tingkat kepercayaan dari suatu entitas ke entitas lain dapat berubah secara dinamik sesuai dengan perubahan performa atau kualitas layananan yang didapatkannya dari entitas lain tersebut.
- Trust is a probabilistic value about an entity: Tingat kepercayaan dapat dikuantisasi dengan ukuran probabilitas pada rentang 0 sampai dengan 1.

- Trust is multidimensional: Dimensi atau atribut-atribut yang digunakan untuk mengukur nilai trust pada suatu bidang bisa dalam jumlah yang besar.
- Trust is personal belief in some entity: Tingkat kepercayaan bersifat subyektif. Setiap orang dapat memiliki latar belakang dan tingkat harapan yang berbeda-beda. Jadi tingkat kepercayaan terhadap suatu entitas yang sama bisa berbeda untuk setiap orang.

3. Components of Trust

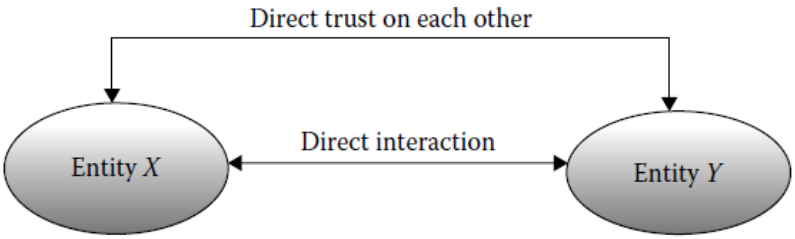
Komponen-komponen dari trust dapat kita kelompokkan ke dalam kategori-kategori berikut:

- Security: Komponen security pada trust terkait dengan tingkat keamanan yang didapatkan dari suatu sistem MCC. Misalnya, sistem keamanan yang diterapkan membuat orang jahat atau yang tidak berhak menjadi sangat sulit atau terlalu mahal secara ekonomi untuk mendapatkan akses ke suatu data atau informasi rahasia.
- Privacy: Komponen ini erat kaitannya dengan teknik atau metode yang digunakan untuk menjaga data pribadi dari kebocoran data ke pihak lain yang tidak berhak.
- Auditability: Komponen auditability terkait dengan kemampuan untuk mengevaluasi atau mendapatkan akses terhadap informasi hasil evaluasi atau audit terhadap suatu organisasi, sistem, proses atau produk.
- Accountability: Komponen trust ini dipengaruhi oleh kepastian bahwa semua operasi yang dilakukan oleh suatu individu, sistem atau proses dapat diidentifikasi secara terpisah dan dapat dilakukan penelusuran terhadap pihak yang bertanggung jawab ketika terjadi suatu kejadian.

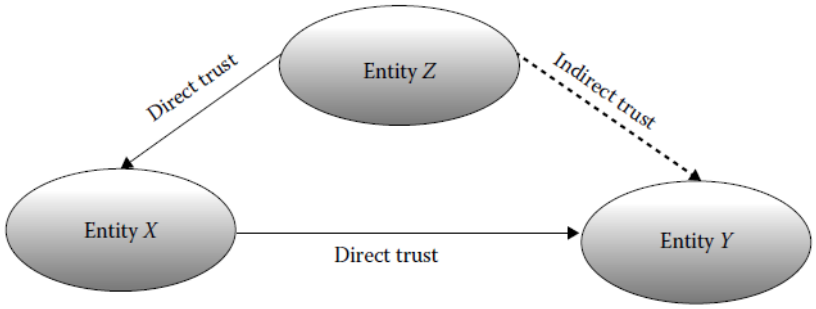
4. Types of Trust

Secara umum, terdapat tiga jenis trust yang dapat terbentuk di antara entitas berbeda:

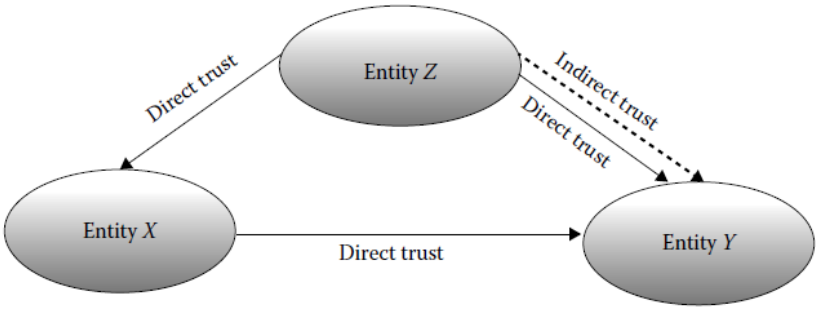
- Direct trust: suatu entitas mempercayai entitas lain secara langsung sebagai hasil dari proses interaksi atau komunikasi yang terjadi secara langsung di antara mereka.



- Indirect trust: suatu entitas dapat mempercai entitas lain secara tidak langsung sebagai hasil dari rekomendasi oleh intitas ketiga. Jenis trust tidak langsung antara dua entitas dibutuhkan ketika kedua entitas belum pernah berinteraksi atau berkomunikasi secara langsung sebelumnya. Jadi nilai trust yang terbentuk berdasarkan hasil observasi dan rekomendasi.



- Hybrid trust: nilai trust hybrid di antara dua entitas ditentukan berdasarkan kombinasi dari pengalaman langsung berinteraksi atau berkomunikasi di antara mereka dan juga berdasarkan hasil rekomendasi dari pihak ketiga.



5. Trust Issues

Trust sulit untuk diwujudkan, tapi mudah untuk hilang. Satu kesalahan dapat merusak kepercayaan yang sudah dibina selama tahunan. Isu-isu trust pada mobile cloud computing biasanya bersumber dari 2 hal, yaitu: rantai trust yang lemah dan kurangnya kontrol dan transparansi. Di antara pengguna dan penyedia layanan cloud terdapat berbagai pihak lain seperti sub-kontraktor. Berbagai sub-kontraktor dibutuhkan untuk memberikan layanan yang cepat kepada para pengguna. Dalam pelaksanaannya sub-kontraktor juga mempekerjakan sub-sub-kontraktor untuk memenuhi kewajibannya. Identitas, reputasi dan tingkat keperyaan

dari masing-masing sub-kontraktor dan sub-sub-kontraktor belum tentu diketahui dengan baik oleh para pengguna maupun penyedia layanan cloud. Bahkan, pengguna juga belum tentu menyadari adanya rantai layanan yang terbentuk di antara pengguna dengan penyedia layanan cloud. Hal inilah yang memunculkan rantai trust yang lemah antara pengguna dengan penyedia layanan cloud.

Isu trust juga bersumber dari kurangnya kontrol dan transparansi. Pengguna tidak mengetahui siapa yang akan memproses informasi pribadinya dan apakah data-datanya sudah mendapatkan pengamanan yang cukup di cloud. Kurangnya control yang dimiliki oleh pengguna dan juga kurangnya transparansi memunculkan ketidakpercayaan dari pengguna ke penyedia layanan cloud. Hal ini dapat mencegah calon pengguna untuk memanfaatkan layanan cloud khususnya ketika melibatkan data dan informasi yang sensitif.

6. Ways of Trust Establishment

Beberapa pendekatan yang dapat dilakukan untuk mengidentifikasi provider layanan cloud (CSP) yang dapat dipercaya:

- Service-level agreement: melalui service level agreement (SLA) yang disetujui antara CSP dan pengguna kita dapat mengetahui layanan apa yang dapat diberikan oleh CSP, fitur-fitur yang terdapat pada layanannya, mekanisme keamanan yang digunakan, kejelasan dan kepastian apa saja yang sudah dipenuhi oleh CSP. Dari informasi-informasi tersebut pengguna dapat memberikan penilaian terhadap tingkat kepercayaan dari CSP tersebut.
- Audit: hasil audit yang dilakukan oleh pihak ketiga terhadap CSP dapat menjadi sumber informasi untuk menentukan tingkat kepercayaan pengguna ke CSP. Banyak standar audit yang tersedia dan CSP yang berbeda bisa menggunakan standar audit yang berbeda pula, seperti: FISMA, SAS70 II, ISO 27001. Hasil audit ini juga dapat dimanfaatkan oleh CSP untuk meyakinkan pengguna akan layanan yang ditawarkannya.
- Measuring and Rating: Tingkat kepercayaan dari suatu CSP juga dapat direfleksikan oleh hasil pengukuran rating yang diberikan oleh para pengguna yang sudah pernah menggunakan layanan dari CSP tersebut melalui suatu survey yang dapat diisi secara online.

- Self-Assessment Questionnaire: suatu organinasi bernama Cloud Security Alliance juga menyiapkan kuesioner yang diberi nama Consensus Assessments Initiative Questionnaire (CAIQ). Kuesioner ini berisi sejumlah pertanyaan yang kemungkinan ditanyakan oleh para pengguna layanan cloud. Kuesioner ini dapat diisi secara mandiri oleh para CSP yang kemudian dipublikasikan ke para pengguna. Kuesioner CAIQ ini juga bisa menjadi salah satu cara untuk menilai kemampuan dan kompetensi yang dimiliki oleh CSP. Hasil kuesioner dapat dimanfaatkan oleh pengguna untuk memberikan penilaian dan perbandingan terhadap layanan yang diberikan oleh pada CSP.
- Trust and Reputation Model: pengukuran tingkat kepercayaan terhadap CSP juga dapat dilakukan melalui suatu model trust dan reputasi. Tingkat kepercayaan dihitung berdasarkan beberapa parameter pengukuran, yang dikenal dengan parameter QoS+, seperti: SLA, tingkat kepatuhan terhadap aturan, lokasi geografi, dukungan terhdap konsumen, performa dari layanan, tingkat keamanan, dan lain-lain. Hasil perhitungan nilai trust ini dapat mendukung pengguna untuk menentukan pilihan CSP yang sesuai sebelum benar-benar berinteraksi dengan layanan CSP.

7. Trust Evaluation

Seperti yang dibahas di bagian sebelumnya, salah satu cara untuk mengukur tingkat kepercayaan dari CSP adalah menggunakan model pengukuran nilai nilai trust. Model ini biasanya mencakup beberapa bagian utama, yaitu: trust representation, trust measurement, dan trust evaluation. Trus representation terkait dengan bagaimana merepresentasikan trust dalam model berdasarkan nilai-nilai parameter yang diukur sebagai input dari model. Kemudian, trust measurement biasanya terkait dengan bagaimana proses pengukuran dari nilai trust dilakukan, termasuk bagaimana nilai dari parameter-parameter input ditentukan. Bagian yang terakhir adalah trust evaluation yaitu proses penerapan model untuk mengevaluasi nilai trust dari suatu CSP. Ada beberapa cara yang dapat ditempuh dalam melakukan trust evaluation terhadap suatu CSP, yaitu:

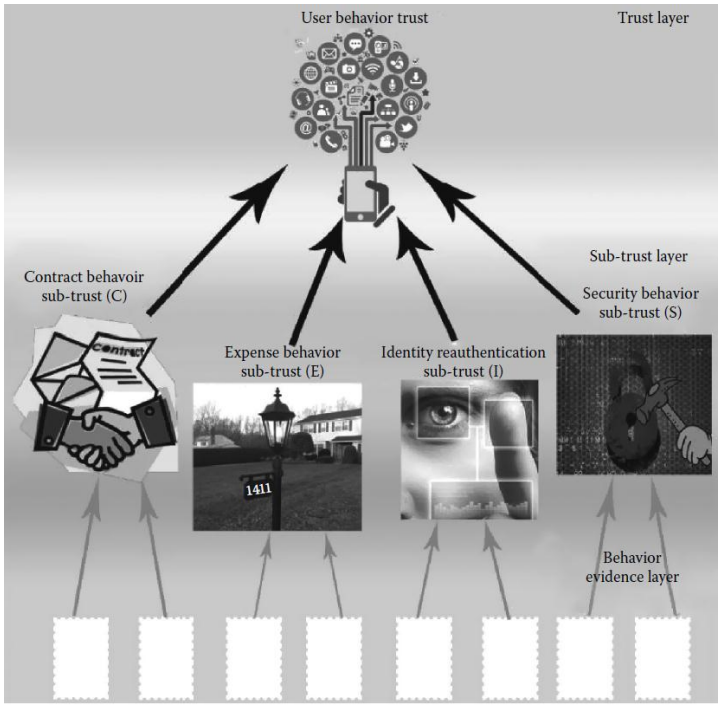
- Black-box approach: nilai atau tingkat kepercayaan dari suatu CSP dievaluasi hanya dengan mempertimbangkan output dari layanan yang dapat diamati. Cara evaluasi ini tidak menggunakan informasi dan pengetahuan terkait dengan arsitektur internal dari sistem atau layanan CSP tersebut.

- Inside-out approach: nilai atau tingkat kepercayaan dari suatu CSP dievaluasi dengan mempertimbangkan arsitektur internal dari sistem yang digunakan oleh CSP termasuk juga kehandalan dari sub-sistem pendukungnya.
- Outside-in approach: nilai atau tingkat kepercayaan dari suatu CSP dievaluasi berdasarkan informasi dan pengetahuan terkait dengan arsitektur internal dari sistem yang digunakan oleh CSP dan komponen-komponen pendukungnya, dan juga dengan mempertimbangkan hasil pengamatan terhadap keseluruhan kualitas layanan yang diberikan.

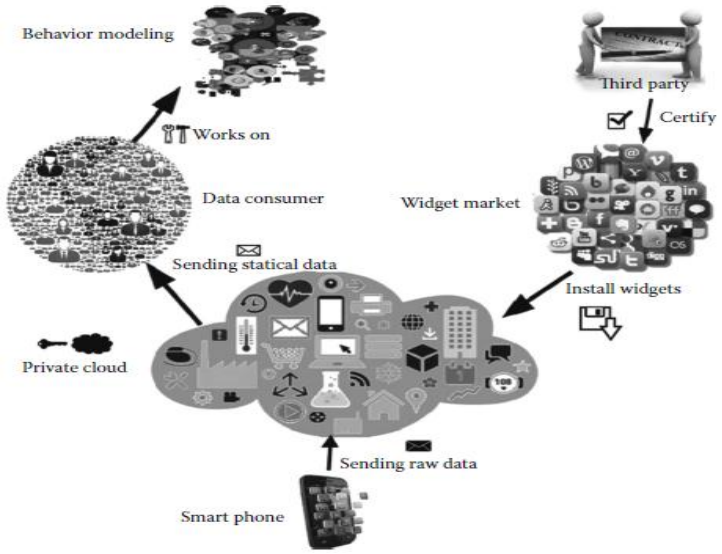
8. Detailed Study of Various Aspects of Trust in MCC

Sejumlah tust framework sudah diusulkan oleh para peneliti untuk mewujudkan rasa saling percaya di antara pengguna dan penyedia layanan cloud. Trust framework yang sudah diusulkan di antaranya:

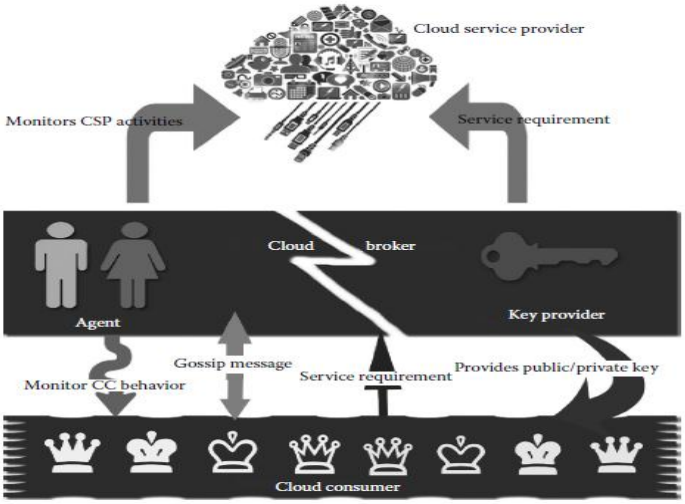
- User Behavior Trust:



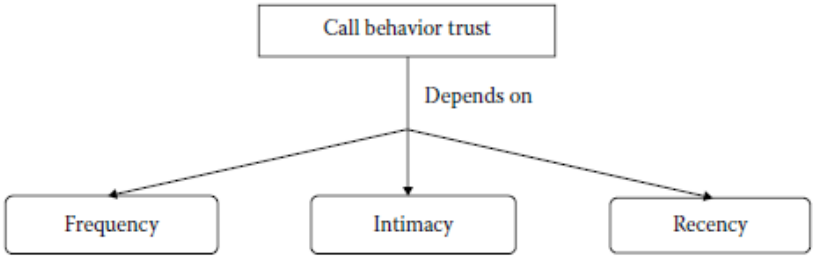
- Trustworthy Mobile Sensing Framework:



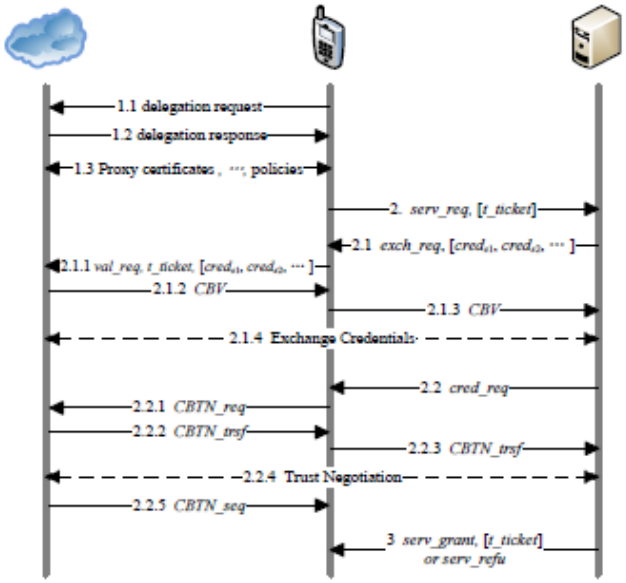
- Mobile Agent-Based Trustworthy Infrastructure:



- Building Trustworthy Social Network Based on Call Behavior:



- Trust-Based Mobile Commerce:



Penjelasan lebih details dari masing-masing trust framework tersebut dapat dibaca pada textbook dan paper-paper terkait.

9. Conclusion

Evaluasi terhadap tingkat atau nilai kepercayaan dari pengguna dan penyedia layanan cloud berlaku dua arah. Evaluasi terhadap tingkat kepercayaan dari penyedia layanan cloud (CSP) sangat penting pagi para pengguna layanan cloud. Hal ini membantu pengguna untuk memilih layanan dari beberapa penyedia layanan yang tersedia, dan juga pengguna dapat menggunakan layanan dengan tingkat keragu-raguan yang lebih rendah khususnya pertanyaan-pertanyaan terkait dengan tingkat keamanan yang diperoleh atas data-datanya. Evaluasi terhadap tingkat kepercayaan dari para pengguna juga tidak kalah pentingnya bagi penyedia layanan cloud (CSP). Hasil evaluasi ini dapat membantu CSP untuk mengeluarkan dan menolak untuk memberikan layanan kepada pengguna-pengguna jahat, dan di sisi lain dapat memberikan layanan yang baik terhadap pengguna-pengguna yang jujur.

DAFTAR PUSTAKA

1. Debashis De. (2015). Mobile Cloud Computing: Architectures, Algorithms and Applications. 01. Chapman and Hall/CRC Press. Florida. ISBN: 9781482242836. Taylor & Francis Publishing ISBN- 978–0–203–88776–9
2. R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, TrustCloud: A framework for accountability and trust in cloud computing, in IEEE World Congress on Services, Washington, DC, pp. 584–588, 2011.
3. J. Golbeck, Computing with trust: Definition, properties, and algorithms, in IEEE Securecomm and Workshops, Baltimore, MD, pp. 1–7, 2006.
4. A. K. Singh, Trust and trust management models for ecommerce & sensor network, International Journal of Engineering Research and Applications, 2(6), 585–619, 2012.
5. K. Govindan and P. Mohapatra, Trust computations and trust dynamics in mobile ad hoc networks: A survey, IEEE Communications Surveys & Tutorials, 14(2), 279–298, 2012.
6. S. Pearson and A. Benameur, Privacy, security and trust issues arising from cloud computing, in Second IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, IN, pp. 693–702, 2010.
7. S. M. Habib, S. Hauke, S. Ries, and M. Muhlhauser, Trust as a facilitator in cloud computing: A survey, Springer Journal of Cloud Computing, 1(1), 1–18, 2012.