BINUS UNIVERSITY ONLINE LEARNING

People
Innovation
Excellence

LECTURE NOTES

MOBI8001 – Mobile Technology & Cloud Computing

Topik 09 - Privacy and Security 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 :

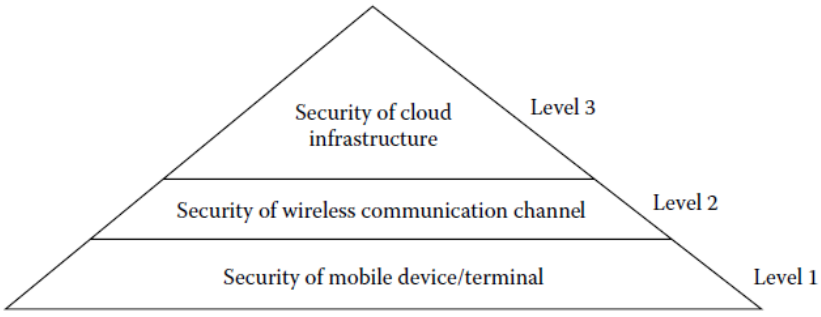
1. Introduction
2. Security Needed in Different Levels for Securing Mobile Cloud Computing
3. Security Issues in Mobile Cloud Environment
4. Conclusion

ISI MATERI

1. Introduction

Beberapa tahun belakangan ini terjadi peningkatan penggunaan smartphone yang sangat drastic. Berdasarkan hasil penelitian yang dilakukan oleh ABI Research, akan terjadi peningkatan jumlah pengguna layanan berbasis cloud dari perangkat mobile dari 1.1% menjadi 19% dari keseluruhan pengguna perangkat mobile hanya dalam kurun waktu 6 tahun. Dalam penelitian yang dilaporkan ini, rentang waktu perkiraan yaitu dari 2008 sampai dengan 2014. Faktor keamanan dari penggunaan smartphone menjadi semakin penting karena melalui smartphone pengguna dapat memperoleh jenis layanan yang semakin yang semakin beragam seperti web browsing, instant messaging , e-commerce, dan lain-lain, termasuk juga penyimpanan data pribadi dan informasi-informasi bernilai ekonomi. Hal ini memancing kehadiran malware pada perangkat mobile yang semakin besar. Dilaporkan telah terjadi peningkatan kehadiran malware pada perangkat mobile sebesar 46% di tahun 2010 dibandingkan dengan tahun 2009. Selain itu, dilaporkan juga sebanyak 74% dari chief information officer (CIO) dan pegawai eksekutive bagian IT merasa enggan dalam mengadopsikan layanan cloud karena resiko penggunaan cloud yang terkait dengan keamanan dan privacy.

2. Security Needed in Different Levels for Securing Mobile Cloud Computing



Resiko keamanan dan privasi pada aplikasi terkait mobile cloud computing perlu dianalisa secara mendalam pada 3 aspek atau level berbeda, yaitu:

1. Level 1: keamanan pada perangkat mobile
2. Level 2: keamanan pada channel komunikasi wireless
3. Level 3: keamanan pada infrastruktur cloud.

Pada level 1, analisa difokuskan pada isu-isu keamanan yang terkait dengan perangkat mobile. Sebagian besar dari perangkat mobile yang ada saat ini menggunakan operating

system terbuka, aplikasi-aplikasi dari pihak ketiga, dan memiliki kemampuan akses wireless dari mana saja dan kapan saja. Karena smartphone saat ini sudah mampu mendukung pemanfaatan aplikasi dan layanan setara dengan PC dan desktop, maka resiko dan ancaman keamanan yang dihadapi oleh smartphone juga sama dengan apa yang terdapat pada PC dan desktop. Isu-isu keamanan pada perangkat mobile dengan contoh-contohnya dirangkum pada tabel berikut.

Security Issues in Mobile Devices with Examples

Security Levels	Security Issues	Examples
Level 1: Mobile devices/ terminal	Information-stealing malwares, spam, phishing, data loss from lost or stolen devices, data leakage from poorly-written applications, vulnerabilities in hardware or OS, unsecured Bluetooth or Wi-Fi	Zimto and NickspyTrojans are information-stealing malwares, fake websites, digital wallet hacking, unwanted message from unknown vendors.

Ada beberapa tindakan dan pendekatan yang dapat dilakukan untuk mengurangi atau mengatasi isu keamanan yang terdapat pada perangkat mobile. Pengguna dapat menjalankan program anti malware pada perangkatnya untuk mengindentifikasi dan menghapus program jahat seperti trojan, virus dan worm. Pengguna juga disarankan untuk melakukan update terhadap OS dan juga hanya mendownload aplikasi dari vendor atau sumber resmi yang sudah dipercaya. Jika perangkat mobile hilang atau dicuri orang, pengguna diharapkan untuk dapat mamanfaatkan fitur atau fasilitas untuk menghapus data dari jarak jauh sehingga data-data yang ada di perangkat tersebut tidak disalah gunakan. Selain itu, teknik enkripsi baik berbasis software atau hardware juga dapat dimanfaatkan untuk melindungi data-data yang ada pada perangkat mobile.

Analisa keamanan pada level 2 terkait dengan pengamanan dari channel komunikasi wireless di antara perangkat mobile dengan server cloud. Perankat mobile mengakses resource dan layanan dari server cloud melalui jaringan komunikasi wireless seperti 3G, Wi-Fi, WiMax, dan Bluetooth. Sejumlah serangan pada jalur komunikasi antara perangkat mobile dan layanan cloud sudah diindentifikasi. Ketika perangkat mobile berkomunikasi dengan cloud, maka mereka rentan terhadap serangan melalui saluran komunikasi. Dengan semakin banyaknya pemanfaatan layanan cloud pada perangkat mobile, maka jumlah dan jenis dari isu keamanan yang terkait dengan channel komunikasi semakin bertambah. Isu-isu keamanan pada channel komunikasi wireless dan contoh-contohnya dapat dilihat pada tabel berikut.

Security Issues in Communication Channel with Examples

Security Levels	Security Issues	Examples
Level 2: Communication channel/mobile network	Access control attacks, confidentiality attacks, integrity attacks, authentication attacks, availability attacks.	War driving, rough APs, MAC spoofing, WEP cracking, Man-In-The-Middle attack, Evil Twin, AP phishing, frame injection, reply attacks, guessing, VPN login cracking, LEAP cracking, DoS, Beacon flood, etc.

Berbagai tindakan atau pendekatan dapat dilakukan untuk mengurangi atau mengatasi resiko kebocoran data ketika ditransmisikan dari perangkat mobile ke server cloud. Penguna perangkat mobile diharapkan untuk mengenkripsi data yang dikirimkan sehingga tidak dapat dibaca oleh pihak lain walaupun data berhasil didapatkan. Juga dianjurkan untuk menggunakan protocol transmisi yang aman seperti HTTPS, VPN maupun penggunaan socket programming untuk mengirimkan data-data sensitif. Keamanan data juga dapat ditingkatkan dengan penggunaan password yang kuat dan juga autentikasi berbasis biometric. Mematikan interface dari komunikasi wireless seperti Wi-Fi dan Bluetooth juga dapat membantu pengamanan dari perangkat mobile.

Isu-isu keamanan pada level 3 merupakan isu-isu penting pada mobile cloud computing yang menjadi penghalang atau alasan bagi banyak pengguna perangkat mobile untuk tidak menggunakan layanan cloud. Ketika pengguna mengirimkan dan menyimpan datanya di cloud, maka mereka kehilangan kontrol akan data tersebut. Peningkatan pemanfaatan layanan cloud dari perangkat mobile juga telah meningkatkan ancaman kemanan pada infrastruktur cloud. Isu-isu keamanan pada infrastruktur cloud dan contoh-contohnya dapat dilihat pada tabel berikut.

Security Issues in Cloud Infrastructure with Examples

Security Levels	Security Issues	Examples
Level 3: Cloud environment	Integrity, digital rights management, virtual machine attacks, phishing, authentication and authorization attacks, platform level attacks	Data and application integrity, pirating and illegal distribution of digital contents, side channel attacks, SQL injection, etc.

Untuk mengurangi atau mengatasi resiko keamanan pada cloud, ada beberapa tindakan atau pendekatan yang dapat dilakukan. Lokasi penyimpanan data harus berada pada lokasi yang terbebas dari isu geopolitical. Sehingga privacy dan keamanan dari data dapat lebih dijaga. Harus tersedia suatu mekanisme untuk merecover data-data pengguna jika terjadi kehilangan data atau data sengaja dihapus oleh penyerang. Selain itu, juga diperlukan

sutau mekanisme key management yang efisien dan aman pada lingkungan cloud. Juga dapat dimanfaatkan teknik autentikasi yang bersifat implisit untuk mengurangi penipuan pada pemanfaatan layanan cloud melalui perangkat mobile.

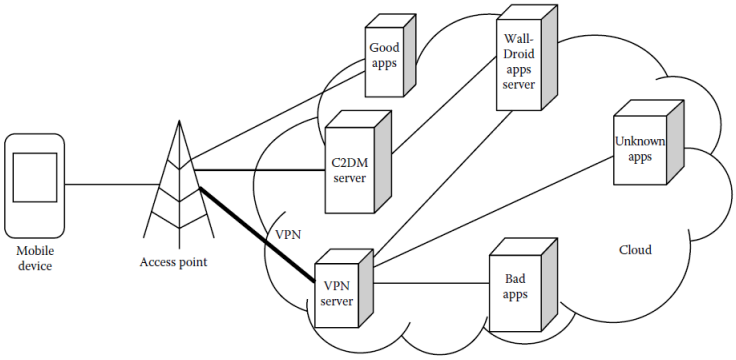
3. Security Issues in Mobile Cloud Environment

Kombinasi antara perangkat mobile dengan infrastruktur cloud telah memunculkan sejumlah isu-isu keamanan. Isu-isu keamanan pada lingkungan mobile cloud secara umum dapat dibagi menjadi dalam 5 kelompok, yaitu:

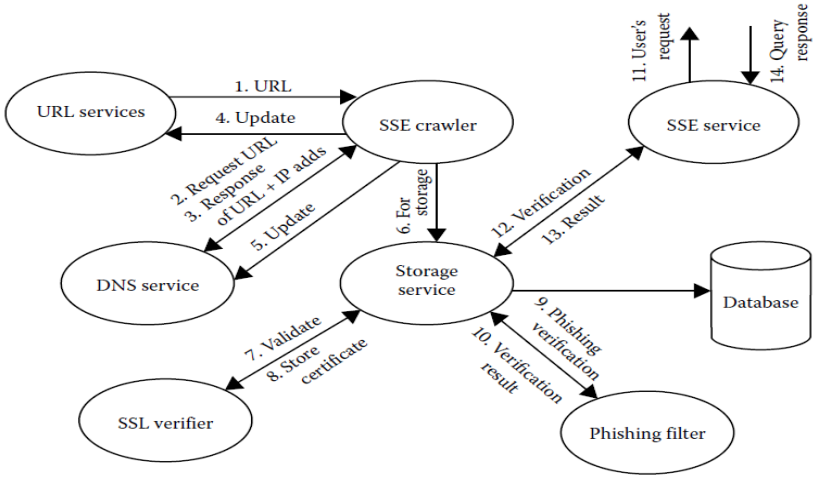
1. Application security
2. Authentication issues
3. Data security
4. Digital rights management
5. Intrusion detection

Berbagai skema keamanan sudah diusulkan oleh para peneliti untuk mengatasi isu-isu keamanan tersebut.

Isu keamanan yang terdapat pada kelompok application security terkait dengan dengan banyaknya aplikasi yang dijalankan pada perangkat mobile. Banyak aplikasi baik dimodifikasi dengan menyusupkan program jahat didalamnya. Aplikasi yang sudah dimodifikasi ini biasanya disebarkan melalui repositori atau sumber-sumber tidak resmi. Aplikasi-aplikasi yang mengandung program jahat dapat membocorkan data pribadi, melakukan panggilan ke nomor telepun premium, atau menjalankan program jahat yang ditriger melalui celah-celah keamanan atau dengan SMS. Sejumlah skema pengamanan sudah diusulkan oleh para peneliti untuk mengatasi isu-isu kemanan yang terkait dengan application security. Dua di antaranya adalah WallDroid dan Secure Search Engine (SSE). WallDroid pada dasarnya adalah firewall untuk aplikasi-aplikasi Android dengan fungsi-fungsi tambahan lainnya. Sedangkan SSE merupakan skema yang ditujukan untuk melindungi pemanfaatan perangkat mobile dari serangan SSL strip-based MITM dan juga dari website phishing.

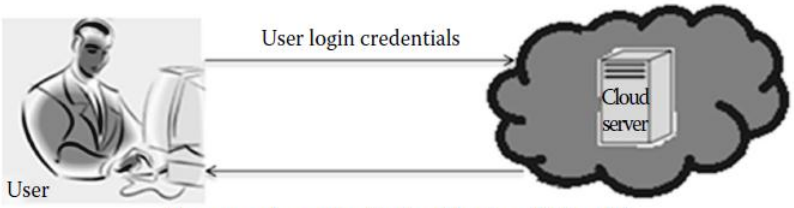


WallDroid



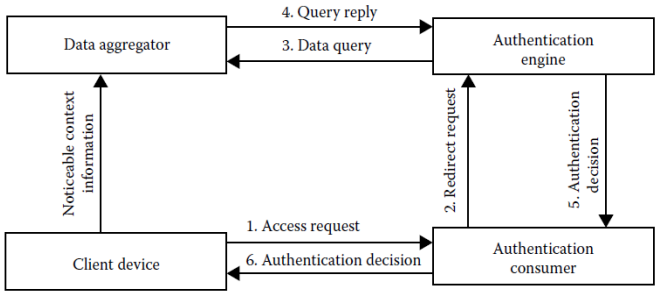
Secure Search Engine (SSE)

Perpindahan dari data-data pribadi dan perusahaan ke cloud memunculkan isu-isu terkait dengan keamanan dan privacy. Protol autentikasi yang handal dibutuhkan untuk memastikan bahwa hanya pengguna yang berhak yang dapat mengakses data-data sensitif tersebut. Pada metode autentikasi tradisional, pengguna biasanya diminta untuk memberikan password oleh server untuk melakukan autentikasi seperti ditunjukkan pada gambar berikut. Proses autentikasi seperti ini rentan terhadap serangan keamanan.

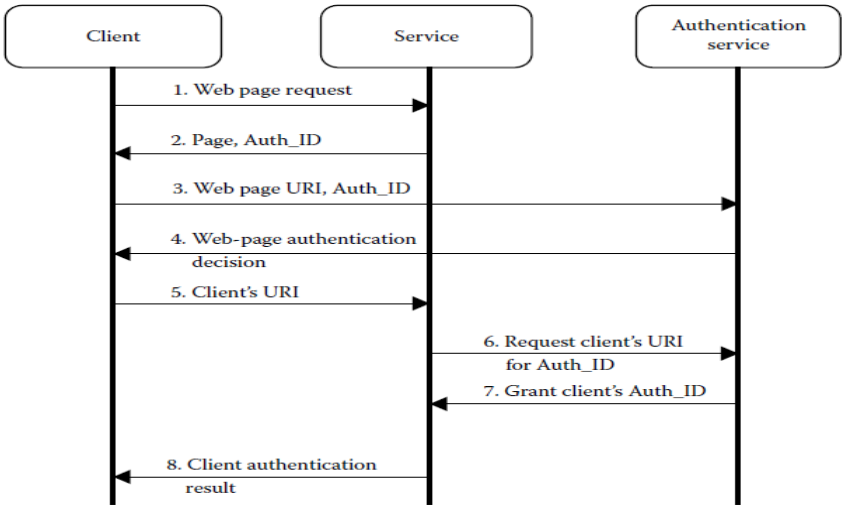


Response after authentication, that is, valid/invalid

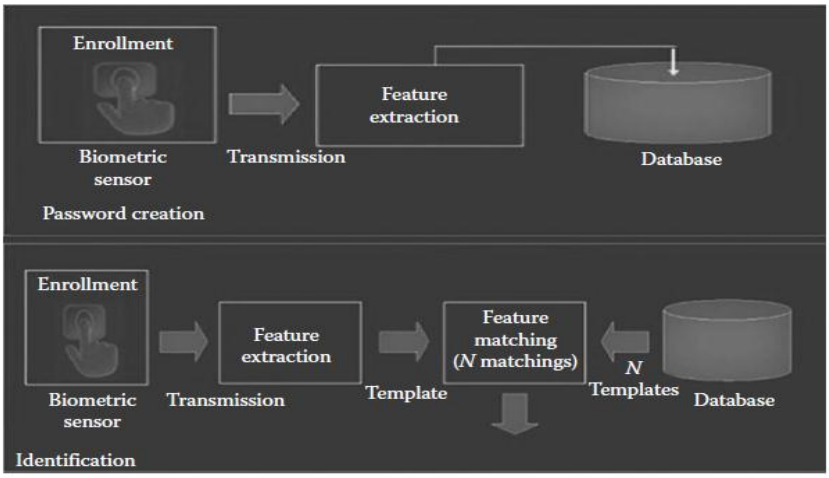
Untuk membuat proses autentikasi menjadi lebih aman maka para peneliti telah mengusulkan beberapa skema autentikasi, misalnya: TustCube, skema autentikasi berdasarkan tindakan atau kebiasaan dari pengguna, SeDiCi 2.0, skema autentikasi yang memanfaatkan teknik zero knowledge proof (ZKP), atau skema autentikasi berbasis biometric. Skema-skema autentikasi dapat diterapkan secara terpisah maupun dikombinasikan untuk meningkatkan tingkat keamanannya.



TrustCube

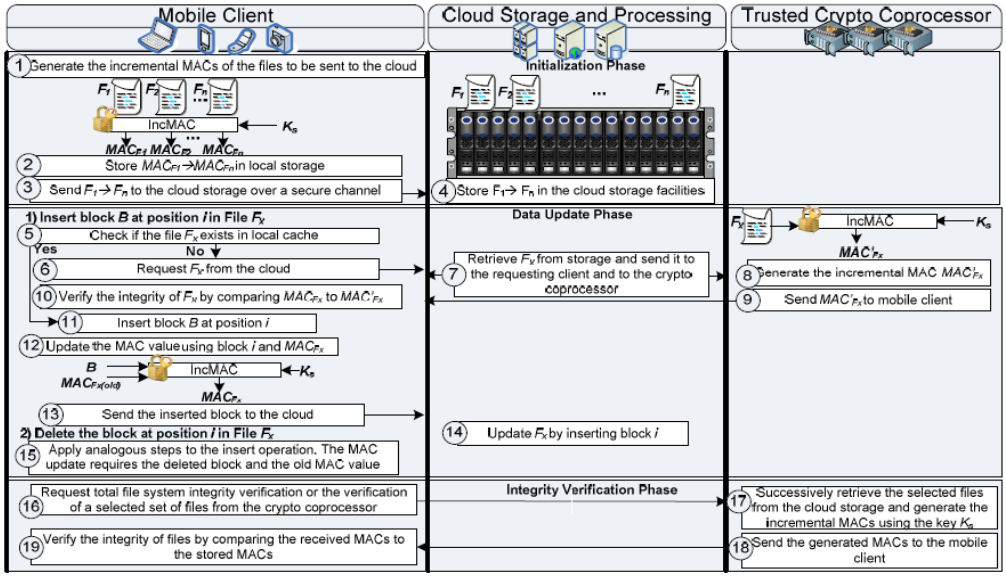


SeDiCi 2.0



Biometric Encryption

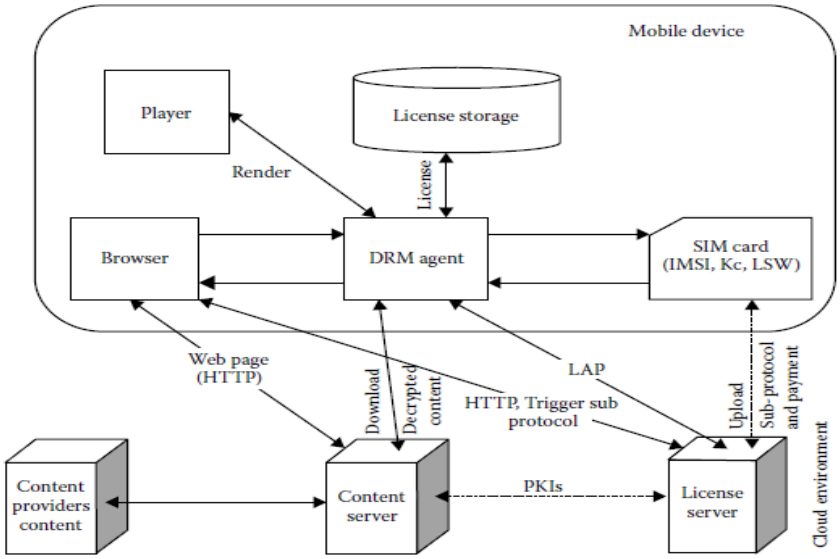
Selain itu, isu-isu keamanan juga terkait dengan Data security. Data-data penting seperti data private, data komersial, data keuangan, dan data perusahaan, dipindahkan dan disimpan di cloud. Kebocoran atas data-data sensitif seperti itu dapat mengakibatkan kerugian secara ekonomi terhadap pengguna atau perusahaan. Jadi diperlukan suatu mekanisme untuk memastikan integritas dari data ketika disimpan di cloud dan data selalu tersedia ketika dibutuhkan. Salah satu skema terkait data security yang sudah diusulkan adalah incremental cryptography berdasarkan Message Authentication Code (MAC). Skema ini dapat digunakan untuk menjaga integritas data ketika disimpan di cloud.



Incremental Cryptography using Message Authentication Code (MAC)

Isu keamanan lainnya terkait dengan digital right management (DRM). Konten-konten digital seperti e-book, gambar, audio, video, dan lain-lain, sekarang banyak disimpan

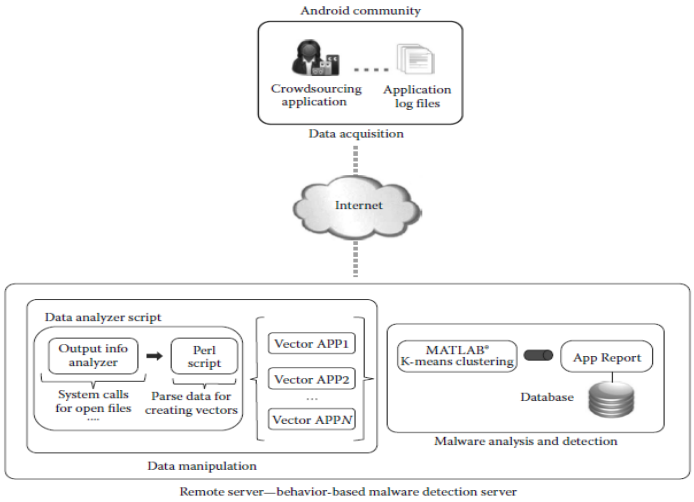
di cloud. Para pengguna perangkat mobile dapat mengakses konten-konten digital tersebut secara mudah dari server cloud melalui jaringan internet. Konten digital dapat dibajak atau didistribusikan secara ilegal oleh pengguna. DRM bertujuan untuk mencegah terjadinya pembajakan ini dan mengatur pemanfaatan dari konten-konten digital. Sistem DRM hanya mengijinkan penguna yang berhak yang memiliki license untuk mengakses konten digital, dan juga mencegah terjadinya pembajakan ataupun pendistribusian konten secara illegal oleh pengguna. Salah satu skema DRM yang sudah diusulkan yaitu Cloud-based SIM DRM (CS-DRM).



CS-DRM

Kelompok isu keamanan pada MCC yang terakhir terkait dengan Intrusion Detection. Smartphone menggunakan arsitektur software yang sama dengan PC, sehingga rentan untuk diserang oleh jenis-jenis virus, worms, malware, atau trojan yang sama. Program-program jahat seperti malware dapat masuk ke dalam smartphone melalui repositori tidak resmi dan menjalankan aktifitas jahatnya pada smartphone. Pengguna dapat memanfaatkan software antivirus untuk mendeteksi dan menghilangkan program-program jahat yang mungkin ada pada smartphonenya. Tapi software antivirus umumnya bekerja berdasarkan suatu signature atau ciri-ciri dari program jahat yang sudah diketahui, yang mana signature tersebut membutuhkan ruang penyimpanan yang cukup besar. Selain ruang penyimpanan, menjalankan program antivirus pada smartphone juga menghabiskan kapasitas CPU dan juga daya batere dalam jumlah besar.

Sedangkan ketersediaan daya komputasi dan batere pada smartphone sangat terbatas. Jadi, solusi untuk menjalankan program antivirus pada smartphone bukanlah suatu solusi yang efisien. Untuk itu, sejumlah skema intrusion detection dengan kebutuhan data komputasi dan batere yang lebih ringan telah diusulkan oleh para peneliti. Skema ini biasanya menggabungkan perangkat mobile dengan komputasi cloud. Salah satu skema intrusion detection yang diusulkan adalah Crowdroid, sebuah sistem deteksi malware pada smartphone berbasis Android.



Crowdroid

Penjelasan lebih details dari skema-skema keamanan yang telah diusulkan oleh para peneliti untuk mengatasi berbagai isu kemanan pada mobile cloud computing dapat dibaca pada textbook dan paper-paper terkait.

4. Conclusion

Pemanfaatan teknologi mobile cloud computing telah memunculkan berbagai ancaman keamanan baik pada sisi perangkat mobile maupun pada sisi cloud. Ancaman-ancaman ini pada umumnya merupakan kombinasi dari ancaman keamanan pada perangkat mobile, jalur komunikasi wireless, dan ancaman pada lingkungan cloud. Untuk memberikan jaminan keamanan pada penerapan mobile cloud computing, para penyedia layanan harus dapat memastikan keamanan dari data, keamanan pada jaringan, integritas dari data, keamanan dari aplikasi, hak akses yang terautentikasi dengan baik, dan jaminan terhadap berbagai faktor-faktor keamanan lainnya.

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. F. S. Gharehchopogh, R. Rezaei, and I. Maleki, Mobile cloud computing: Security challenges for threats reduction, International Journal of Scientific and Engineering Research, 4(3), 8–14, 2013.
3. S. K. V. Ko, J. H. Lee, and S. W. Kim, Mobile cloud computing security considerations, Journal of Security Engineering, 9(2), 143–150, 2012.
4. S. Hui, Z. Liu, J. Wan, and K. Zhou, Security and privacy in mobile cloud computing, in Ninth International Wireless Communications and Mobile Computing Conference, Sardinia, Italy, pp. 655–659, 2013.
5. M. S. Morshed, M. M. Islam, M. K. Huq, M. S. Hossain, and M. A. Basher, Integration of wireless hand-held devices with the cloud architecture: Security and privacy issues, in International Conference on Parallel, Grid, Cloud and Internet Computing, Barcelona, Spain, pp. 83–88, 2011.