Desain E-*Health*:

Sistem Keamanan Aplikasi E-*health* Berbasis *Cloud Computing* Menggunakan Metode *Single Sign On*

Erika Ramadhani

Jurusan Teknik Informatika Universitas islam Indonesia
Jl. Kaliurang km 14 Yogyakarta 55510
Telp (0274) 895287 ext 122, fax (0274) 895007 ext 148
erika@uii.ac.id

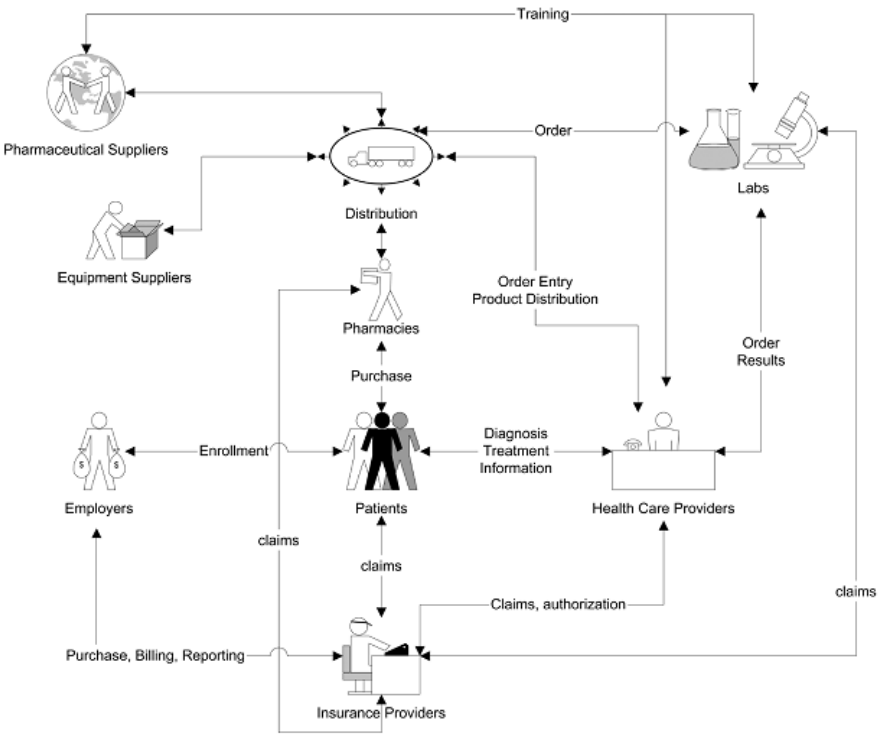
Abstract. Salah satu jenis pelayanan kesehatan yang sedang berkembang saat ini adalah e-health. E-health memanfaatkan teknologi elektronik dan internet dalam pertukaran data. Berdasarkankan pada kompleksitas kebutuhan sistem pelayanan kesehatan dan teknologi internet yang semakin pesat menyebabkan e-health diintegrasikan dengan cloud computing. Teknologi cloud computing merupakan teknologi yang memudahkan konsumen untuk mengakses layanan cloud melalui web browser atau layanan web. Pada umumnya aplikasi berbasis web merupakan salah satu contoh layanan SaaS (*Software as a Service*) yang dimanfaatkan untuk e-health. Terdapat banyak isu keamanan pada cloud computing. Masalah keamanan yang bisa terjadi adalah *XML Signature Elemen Wrapping, Browser Security, Cloud Malware Injection Attack, dan Flooding Attacks*. Namun isu keamanan difokuskan dari sisi pengguna, karena kehilangan atau kebocoran data dan pembajakan *account* atau *service* merupakan ancaman yang sangat krusial bagi pengguna. Salah satu cara untuk mengamankan kehilangan data dan pembajakan *account* tersebut adalah dengan melakukan *identity management* dan *access control*. Metode single sign on merupakan salah satu solusi *identity management*. Hasil akhir dari penelitian ini adalah sebuah aturan untuk melindungi keamanan data aplikasi e-health. Beberapa aturan yang digunakan adalah proses login dengan menggunakan otentikator, jalur komunikasi yang dilindungi dengan menggunakan enkripsi, serta manajemen identitas untuk pemberian hak akses terhadap aplikasi e-health.

***Keywords*:** e-*health*, sistem keamanan, *single-sign-on*

1 Pendahuluan

E-*health* merupakan jenis pelayanan kesehatan yang memiliki pertukaran informasi yang sangat kompleks. Kompleksitas e-*health* bisa dilihat pada layanannya, yakni: *content*, *commerce*, *connectivity*, dan *care*[1]. Gambar 1 menunjukkan beberapa pihak yang terlibat dan interaksinya pada jaringan pelayanan kesehatan. Dapat dilihat bahwa kompleksnya alur bisnis, data, dan informasi pada e-health.. Terdapat banyak pihak yang terhubung melalui e-health. Bisa dipastikan kompleksnya pertukaran informasi pada sistem e-health. Sehingga e-health diintegrasikan dengan cloud computing untuk menghemat sumber daya dan memudahkan dalam pertukaran informasinya.

E-health yang terintegrasi dengan teknologi cloud computing bisa berupa apliksi yang diakses dengan menggunakan web browser atau layanan web. Layanan ini disebut sebagai *Software as a Service* (SaaS) pada cloud computing.



Gambar 1. Jaringan pelayanan kesehatan[1]

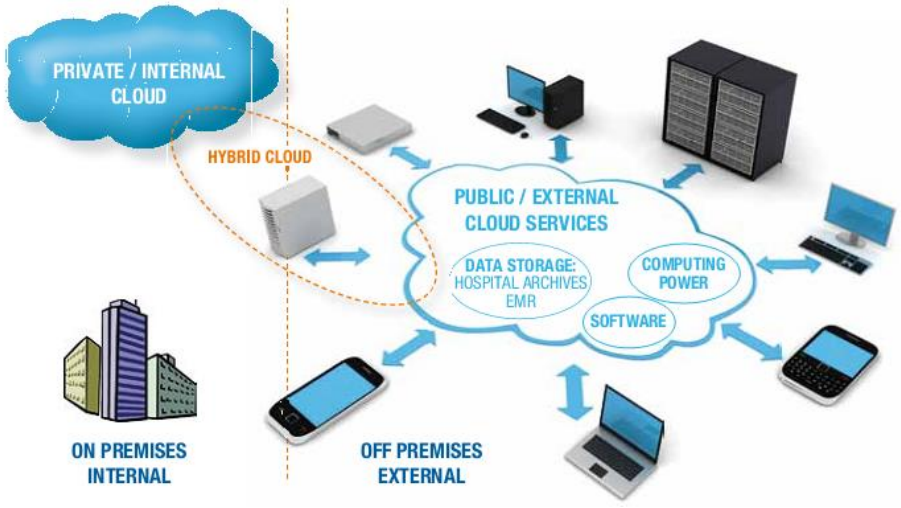
Berdasarkan pada gambar 1 maka sistem keamanan dan privasi pada e-health perlu diperhatikan, khususnya pada layanan aplikasi yang terintegrasi pada cloud computing. Salah satu metode yang digunakan dalam keamanan data aspek autentikasi dan otorisasi pada aplikasi atau layanan cloud computing adalah teknologi *single-sign-on*. Teknologi *single-sign-on* (SSO) merupakan teknologi yang memberikan izin pengguna jaringan agar dapat mengakses sumber daya di dalam jaringan dengan menggunakan satu akun pengguna. Teknologi ini sangat cocok digunakan karena e-health merupakan jaringan yang sangat besar dan bersifat heterogen dan bisa diintegrasikan dengan cloud computing. Dengan menggunakan SSO, seorang pengguna melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang ada didalam jaringan.

Dalam paper ini akan dibahas bagaimana keamanan dari sisi SaaS cloud computing e-health dengan menggunakan metode SSO. Keluaran dari paper ini adalah akan

diberikan cara kerja, skenario, dan desain implementasi SSO di e-health. Sehingga dihasilkan aturan penggunaan aplikasi e-health oleh seorang pengguna.

2 *Cloud Computing*

Cloud computing merupakan komputasi berbasis internet. Server cloud computing menyediakan daya, penyimpanan, pengembangan platform, atau perangkat lunak terhadap komputer atau perangkat yang meminta pelayanan cloud computing. Cloud computing memiliki beberapa layanan, yakni: *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), dan *Software as a Service* (SaaS). Seorang pengguna bisa menggunakan aplikasi berbasis web melalui web browser tanpa harus melakukan instalasi aplikasi pada perangkat komputernya. Terdapat beberapa macam jenis cloud computing, diantarnya adalah *public cloud*, *private cloud*, dan *hybrid cloud*.

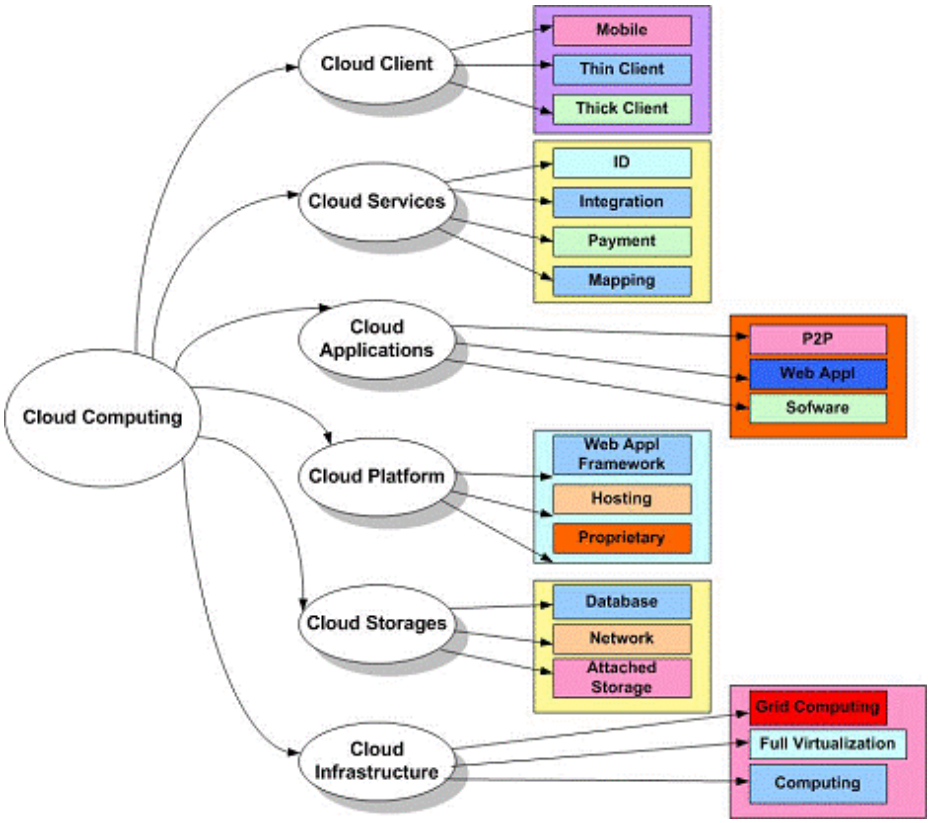


Gambar 2. *Cloud computing* pada layanan kesehatan[6]

3 *Software as a Service*

Struktur *cloud computing* ditunjukkan pada gambar 3. *Software as a Service* (SaaS) merupakan kemampuan cloud computing untuk memberikan layanan kepada pengguna. Layanan yang diberikan ini berupa aplikasi yang dijalankan diatas infrastruktur cloud computing. Terdapat tiga komponen platform yakni *computer desktop*, *mobile devices*, dan cloud, dengan memperhatikan masalah kemudahan dan keamanan, dimungkinkan dapat dengan mudah para pengguna untuk pindah dari satu aplikasi ke aplikasi lain dimana saja[7]. Berdasarkan pada komponen platform yang

heterogen, maka SaaS diharapkan dapat mengintegrasikan beberapa perangkat dan manajemen *tools* yang ada.



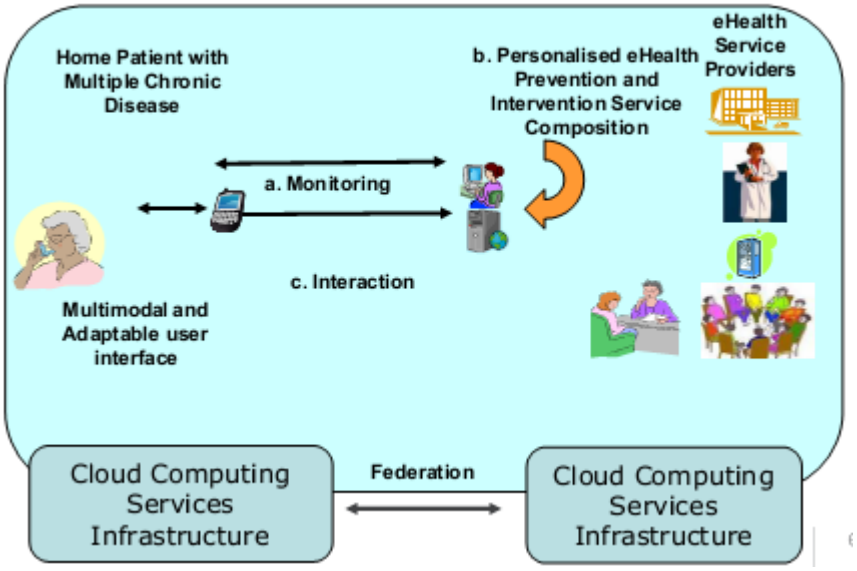
Gambar 3. Struktur *cloud computing*[7]

Adanya SaaS ini memudahkan dalam pertukaran informasi di sebuah sistem, salah satunya e-health. Pada sistem e-health terdiri atas tiga aplikasi utama: aplikasi pasien, aplikasi dokter rujuk, dan aplikasi *expert* dokter[3].

4 Keamanan Pada E-*health*

Privasi pasien dan informasi kesehatan wajib dilindungi. Hal ini dikarenakan pasien tidak mungkin berbagi informasi yang sangat pribadi kecuali mereka percaya bahwa data mereka dilindungi kerahasiaannya. Kompleksitas alur pertukaran informasi dan data pada e-health menyebabkan e-health sangat rentan terhadap ancaman-ancaman keamanan sistem e-health. Gambar 4 menunjukkan skenario e-health yang terdiri atas 3 poin penting yakni monitoring, pencegahan personal e-health, komposisi intervensi

layanan dan interaksi. Isu utama yang perlu diperhatikan pada sistem e-health adalah proteksi data (privasi), kerahasiaan, properti, dan pelayanan *outsource*[2].

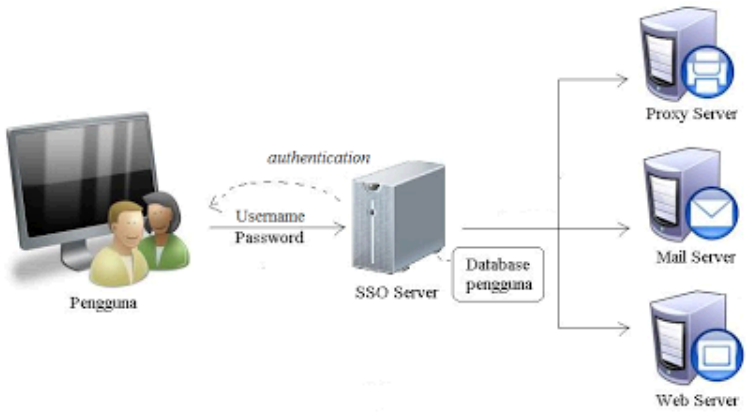


Gambar 4. Skenario e-*health*[2]

Ukuran keamanan data dilihat dari integritas data, manajemen identitas, dan kontrol akses[8].Untuk mendapatkan data yang konsisten dan valid maka integritas data harus diperhatikan. Enkripsi tidak hanya digunakan untuk proses pertukaran data, tetapi pada saat penyimpanan data juga harus diperhatikan. Akses kontrol digunakan untuk mengontrol siapa saja yang terlibat pada jaringan e-*health*, untuk menghindari akses ilegal terhadap sistem.

5 *Single Sign On* (SSO)

SSO merupakan sistem otentikasi terhadap pengguna yang mana seorang pengguna melakukan login cukup satu kali saja untuk mengakses beberapa aplikasi. Sistem SSO yang biasa adalah seorang pengguna melakukan proses login berulang kali untuk satu aplikasi yang akan diakses. Sistem single sign on yang lainnya adalah proses login dilakukan cukup satu kali untuk mengakses beberapa aplikasi yang ditunjukkan pada gambar 5. Pada implementasinya, sebuah sistem SSO akan menyimpan *credentials* dalam sebuah server terpusat atau sebuah direktori. Sistem direktori tersebut harus mampu menjaga kestabilan sistem dalam mereplikasi penyimpanan *credential*. Untuk melakukan hal tersebut, maka sistem harus memiliki metode yang baik untuk penyimpanan *credential*.



Gambar 5. Sistem SSO

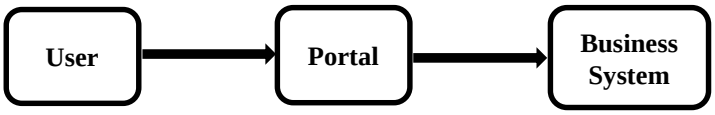
Lightweight Directory Access Protocol (LDAP) mampu melakukan *update* dan mencari direktori yang berjalan pada sebuah jaringan TCP/IP. LDAP merupakan sebuah protokol servis direktori. SSO biasanya terintegrasi dengan sebuah LDAP direktori, sehingga dapat bekerja dengan efektif.

6 Hasil Analisa

Sistem keamanan yang akan digunakan pada aplikasi e-health berbasis cloud computing adalah manajemen identitas dengan menggunakan teknologi SSO. Produk SSO yang digunakan adalah *Security Assertion Markup Language* (SAML) yang menghubungkan antara pengguna dengan aplikasi web dalam bentuk portal. SAML merupakan standar yang mendefinisikan kerangka berbasis XML untuk menggambarkan dan bertukar informasi keamanan antar mitra bisnis secara online[5]. Otentikasi SSO dengan menggunakan SAML akan memberikan keamanan proses pertukaran dan identifikasi data berbasis XML[4].

Skenario yang digunakan adalah terdapat sebuah puskesmas dengan nama PuskesmasTegalsari, yang memiliki 60 pegawai. Puskesmas tersebut melayani pencatatan data pasien, rujukan dokter, rujukan rumah sakit, dan lain-lain. Pada puskesmas tersebut terdapat intranet yang berisi sebuah paket website untuk pencatatan data pasien, pencatatan rujukan dokter, pencatatan penggunaan obat, dan lain-lain. Semua paket aplikasi dibuat dalam bentuk private cloud computing sebagai portal perusahaan yang mengaplikasikan SSO dan proteksi akses menggunakan SAML.

Analisa akan diawali dengan aturan komunikasi dengan menggunakan *web single sign on* yaitu otentikasi permintaan pelayanan web. Ilustrasi web single sign on bisa dilihat pada gambar 6.

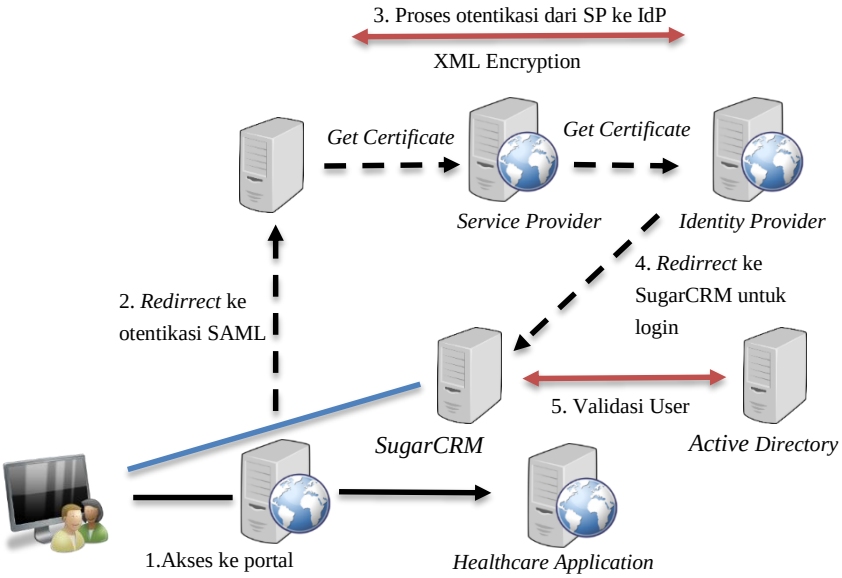


Gambar 6. Rancangan sistem keamanan *web single sign on*

Berdasarkan pada gambar 6 rancangan sistem keamanan web single sign on adalah sebagai berikut:

1. Pada langkah awal, pengguna melakukan otentikasi melalui sistem yang berupa portal.
2. Aplikasi portal akan melakukan pemanggilan layanan web menuju *business system*.
3. Aplikasi yang berada pada portal menggunakan *username/password* yang sama untuk memanggil *business system*.

Berdasarkan pada aturan komunikasi diatas, seorang pengguna apabila ingin mengakses sebuah aplikasi berbasis web, maka dia harus melakukan proses login. Setelah melakukan proses login ini, maka sebuah otentikator akan melakukan otentikasi. Bila pengguna berhasil melakukan otentikasi, maka pengguna tersebut dapat menggunakan layanan yang disediakan oleh jaringan.



Gambar 7. Rancangan sistem keamanan *web single-sign-on*

Pada gambar 7 merupakan sebuah rancangan sistem keamanan aplikasi berbasis cloud computing pada e-health. Seorang pengguna akan melewati portal terlebih dahulu untuk melakukan login *username* dan *password*. Proses login ini yang disebut dengan SSO. Proses otentikasi SSO dilakukan dengan menggunakan metode SAML, yang mana jalur otentikasi diberikan enkripsi XML. SugarCRM merupakan antarmuka

pengguna sebagai terget layanan yang melihat jalannya SSO. Sedangkan *active directory* merupakan sistem yang difungsikan untuk mengatur hak askes pengguna dan komputer. Berikut adalah *tools* bisa digunakan:

1. OpenSSO, yakni manajemen akses web open source yang mengimplementasikan keamanan web service. OpenSSO bertindak sebagai Service Provider (SP).
2. SimpleSAMLphp, merupakan aplikasi native PHP yang bekerja di beberapa protokol dan mendukung mekanisme autentikasi. SimpleSAMLphp bertindak sebagai Identity Provider (IdP).
3. SugarCRM, merupakan aplikasi berbasis CRM yang berbasis PHP.
4. Lightweight Directory Access Protocol (LDAP) merupakan protokol *active directory* untuk mengakses suatu *directory service*.

Tujuan dari rancangan ini adalah untuk mengamankan data sari sisi user. Maka sistem keamanan penggunaan aplikasi e-health dilakukan secara bertahap, dari sisi otentikasi, jalur otentikasi, pengaturan hak akses, dan penggunaan aplikasi e-health yang sudah terintegrasi. Keuntungan menggunakan sistem ini adalah sistem bersifat murah dan bisa dikembangkan secara mandiri.

7 Kesimpulan

Sistem keamanan pada jaringan e-*health* sangat diperlukan. Sistem keamanan ini digunakan untuk mengatur penggunaan aplikasi e-health berbasis cloud computing agar privasi dan integritas data terjamin keaslian dan keamanannya. Data yang tercatat pada sebuah pelayanan kesehatan khususnya puskesmas hanya boleh diketahui oleh tenaga medis atau dokter. Manajemen identitas atau pengguna terutama penggunaan teknologi SSO sangat membantu dalam menjaga privasi dan integritas data. Teknologi SSO yang digunakan ini adalah teknologi keamanan sistem yang melindungi dari sisi proses login, proses pengiriman data, dan pengaksesan data.

8 Pustaka

1. Bliemel, M. Hassanein, K. (n.d.). E-health : applying business process reengineering principles to healthcare in Canada Michael Bliemel and Khaled Hassanein *, x(x), 1–19.
2. Centre, C. (2010). Cloud Computing for, (July), 1–11.
3. eHealthopinion. (n.d.). . Retrieved October 6, 2015, from http://ehealthopinion.com/Saas.aspx
4. Lewis, K., Lewis, J. E., & Ph, D. (2009). Sign- Web Single Sign - On Authentication using SAML, 2(1), 1–8.
5. Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., & Scavo, T. (2007). Security Assertion Markup Language (SAML) V2.0 Technical Overview (OASIS). May, (February), 50. Retrieved from https://www.oasis-open.org/committees/security/docs/draft-sstc-baker-saml-arch-00.pdf
6. Recommendations, C. (2012). Advancing healthcare delivery with cloud computing 2, 7–17.
7. Stiawan, D. (n.d.). Paradigma Baru, 1–6.
8. Veneto, C. (n.d.). CLOUD COMPUTING FOR E - HEALTH DATA PROTECTION ISSUES & Intro : Challenges High quality services are to be delivered.