# PENILAIAN PRESTASI PERKHIDMATAN WEB YANG SELAMAT DENGAN MENGGUNAKAN KAEDAH PELBAGAI LAPISAN KOMUNIKASI DALAM E-KESIHATAN

Nor Hanim Che Hassan
Rossilawati Sulaiman

*Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia*

**ABSTRAK**

Penggunaan maklumat dan teknologi komunikasi (ICT) dalam bidang perkhidmatan kesihatan bukan sesuatu yang baru. Penggunaan ICT dalam bidang kesihatan telah membantu profesional menambahbaik kecekapan dan keberkesanan perkhidmatan. Inisiatif ICT dalam perkhidmatan kesihatan juga dikenali sebagai e-kesihatan menyediakan banyak kelebihan seperti kecekapan dalam merekod dan menempatkan maklumat penting dengan cepat, kos yang lebih efektif serta perluasan skop perkhidmatan kesihatan yang melangkau sempadan geografi. Dalam kes ini, kaedah komunikasi yang digunakan adalah sangat penting. Kaedah yang sering digunakan adalah dengan menggunakan perkhidmatan web kerana ia boleh saling bertukar mesej antara aplikasi-aplikasi yang berbeza dan platform yang berlainan. Sejajar dengan penggunaan perkhidmatan web yang meluas melalui internet, ancaman keselamatan terhadap perkhidmatan web juga semakin meningkat. Oleh yang demikian, aspek keselamatan perlu dititikberatkan untuk memastikan bahawa perkhidmatan web dilindungi dari serangan terutama apabila melibatkan maklumat sensitif dalam bidang kesihatan. Teknologi penyelesaian permasalahan sedia ada tidak menyediakan keselamatan yang fleksibel untuk memenuhi keperluan komunikasi yang berbeza dengan menggunakan perkhidmatan web. Kajian ini fokus terhadap keselamatan perkhidmatan web dengan menggunakan kaedah pelbagai lapisan komunikasi dalam bidang e-kesihatan yang menggunakan lima jenis lapisan komunikasi yang berbeza. Kriptografi merupakan satu mekanisma keselamatan yang penting bagi memastikan kerahsiaan dan integriti maklumat dalam komunikasi antara dua pihak. Kaedah dalam kriptografi yang digunakan dalam kajian ini adalah teknik penyulitan. Teknik ini memainkan peranan bagi memastikan kerahsiaan semasa proses pertukaran mesej. Oleh yang demikian, perkhidmatan web yang mengaplikasikan penggunaan pelbagai lapisan keselamatan dengan teknik penyulitan algoritma simetri, Advanced Encryption Standard (AES) 128 bit, 192 bit dan 256 bit telah dibangunkan. Perbandingan dibuat bagi menilai prestasi masa pemprosesan dengan atau tanpa penyulitan bagi setiap lapisan. Hasil kajian menunjukkan kos overhed bagi lapisan pertama iaitu dengan penyulitan adalah lebih tinggi berbanding lapisan lain. Walau bagaimanapun, ciri keselamatan ke atas perkhidmatan web perlu ditoleransi dengan pemprosesan masa yang lebih perlahan bagi memastikan keselamatan maklumat.

Kata kunci: Komunikasi pelbagai lapisan, perkhidmatan web, penyulitan, keselamatan

ABSTRACT

*The use of information and communication technology (ICT) in the field of health services is not something new. ICT in health professional has helped improve the efficiency and effectiveness of the services. ICT initiatives in the health services, also known as e-health provides many advantages such as efficiency in recording and put important information quickly, more cost-effective as well as expanding the scope of health services that beyond geographical boundaries. In this case, the method of communication used is very important. Web service is often used because it can mutually exchange messages between different applications and different platforms. In line with the widespread use of web services through the internet, web services security threats are also increasing. Therefore, the security aspect needs to be considered to ensure that web services are protected from attacks, when sensitive information are involved especially in the field of health. Technological of existing solutions do not provide the security that is flexible to meet the needs of different communications using web services. This paper focuses on the security of web services using the multi-layer communication approach in the field of e-health. Cryptography is an important security mechanism to ensure the confidentiality and integrity of information in the communication between the two parties. Cryptographic methods used in this study is the encryption technique. This technique plays a role to ensure confidentiality during the process of exchanging messages. Thus, a web service that applies the use of multiple layers*

*of security with encryption techniques symmetric algorithm, Advanced Encryption Standard (AES) 128 bits, 192 bits and 256 bits has been developed. Comparison is made to evaluate the performance of the processing time with or without encryption in each layer. The result shows the overhead of web servicesin Layer 1 encryption is higher than web services without encryption in the other layer. However, the security features on web services should be tolerated with a slower processing time to ensure the security of information.*

*Keywords: Multilayer communication,web services, encryption, security*

## PENGENALAN

Penggunaan maklumat dan teknologi komunikasi (ICT) dalam bidang penjagaan kesihatan bukan sesuatu yang baru. Ia menjanjikan kualiti penjagaan yang lebih baik kepada pesakit, menyediakan pembangunan professional yang berterusan, mempromosikan pertukaran data dan maklumat kesihatan serta menyokong persekitaran kajian kesihatan (Baroud, 2008). World Health Organization (WHO) telah mendefinisikan e-kesihatan sebagai penggunaan ICT secara kos efektif dan selamat dalam menyokong kesihatan dan bidang berkaitan kesihatan termasuk perkhidmatan penjagaan kesihatan, pengawasan kesihatan, literatur kesihatan dan pendidikan, ilmu serta kajian kesihatan. Pelaksanaan e-kesihatan telah memberi kesan perubahan yang luar biasa di negara membangun. Skop teknologi e-kesihatan juga melangkau sempadan geografi (Anshari, M. et al 2012). Dalam kes ini, kaedah komunikasi yang digunakan antara pihak yang terlibat adalah sangat penting.

Perkhidmatan web merupakan salah satu cabang teknologi yang membolehkan komunikasi antara dua pihak dijalankan melalui internet. Perkhidmatan web menyediakan satu pendekatan standard bagi aplikasi perisian yang berbeza melibatkan perolehan maklumat semasa (*real-time)* kepada pengguna (Chen et al 2003). Dalam bidang kesihatan, maklumat pesakit, penyakit, ubat-ubatan merupakan maklumat kritikal yang perlu dirahsiakan dari pihak yang tidak berkenaan. Maklumat kesihatan adalah sensitif dan kritikal, dan kebergantungan yang tinggi terhadap rekod yang boleh dipercayai, isu kebolehpercayaan, keselamatan dan privasi adalah signifikan dan mesti ditangani dengan jelas dan efektif. Walau bagaimanapun, keselamatan sering menjadi kebimbangan yang jelas dalam pengadaptasian perkhidmatan web (Chen et al 2003).Pelbagai ancaman keselamatan dalam teknologi web wujud seiring dengan peningkatan teknologi.

Teknologi penyelesaian permasalahan sedia ada bagi keselamatan perkhidmatan web adalah dengan menggunakan *Secure Socket Layer* (SSL), spesifikasi WS- Security dan penyulitan XML. Walau bagaimanapun, jika sesebuah organisasi memerlukan keselamatan yang fleksibel untuk memenuhi keperluan komunikasi yang berbeza dengan menggunakan perkhidmatan web, teknologi sedia ada tidak dapat memenuhi keperluan tersebut. Kajian oleh Rossilawati et al (2011) bagi menyelesaikan masalah ini adalah dengan menggunakan kaedah pelbagai lapisan komunikasi. Penyelesaian tersebut menggunakan teknologi Sistem Multiagen (MAS). Oleh itu, kajian ini mencadangkan untuk menggunakan kaedah pelbagai lapisan komunikasi ke atas perkhidmatan web.

Objektif kajian ini adalah untuk membangunkan satu persekitaran keselamatan yang fleksibel dengan menggunakan kaedah pelbagai lapisan komunikasi dengan menggunakan perkhidmatan web dalam bidang e-kesihatan dan membandingkan tahap prestasi keselamatan di setiap lapisan komunikasi yang menggunakan perkhidmatan web.

Dalam bab seterusnya akan diterangkan hasil kajian literatur yang telah dibuat. Kemudian bab seterusnya pula akan menerangkan metodologi kajian yang digunakan bagi membuktikan konsep kajian ini. Seterusnya, adalah pembentangan keputusan dan analisis yang telah dibuat

hasil dari kajian ini. Bab terakhir merupakan kesimpulan dari keseluruhan kajian serta cadangan kajian lanjut yang boleh dilaksanakan.

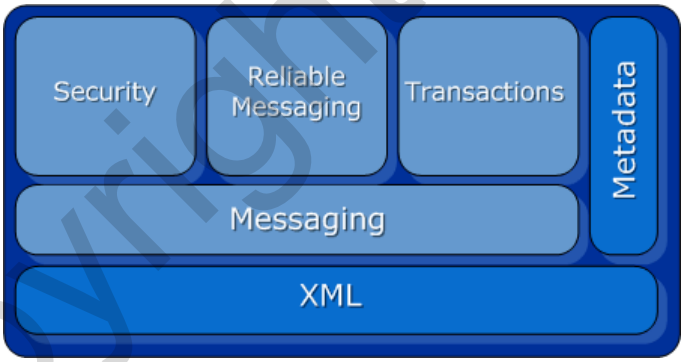
## KAJIAN LITERATUR

Bahagian ini menyoroti literatur tentang perkhidmatan web, e-kesihatan, kajian keselamatan dan jurang kajian ini dengan kajian sedia ada.

### PERKHIDMATAN WEB

Menurut World Wide Web Consortium (W3C), perkhidmatan web adalah sistem perisian yang direka untuk menyokong interaksi saling boleh kendali mesin kepada mesin lain melalui rangkaian. Ia mengandungi antaramuka yang diterangkan dalam format yang boleh diproses oleh mesin (secara spesifiknya *Web Service Description Language* (WSDL)). Sistem lain berinteraksi dengan perkhidmatan web dalam kaedah yang telah ditetapkan dengan menggunakan mesej *Simple Object Access Protocol* (SOAP), lazimnya disampaikan dengan menggunakan *Hypertext Transfer Protocol* (HTTP) dengan penerbitan *Xtensible Markup Language* (XML) berhubung dengan standard berkaitan web lain.

Dalam erti kata lain, perkhidmatan web adalah satu fungsi yang boleh diakses oleh program lain melalui web. Contohnya adalah mekanisma permintaan dan respons yang membenarkan pelanggan untuk mengakses atau mengubah data dari jarak jauh. Standard formal bagi perkhidmatan web adalah protokol SOAP yang yang membawa mesej XML sebagai format data (Brekken & Asprang 2006). Rajah 1 memaparkan garis panduan komponen perkhidmatan web oleh IBM.

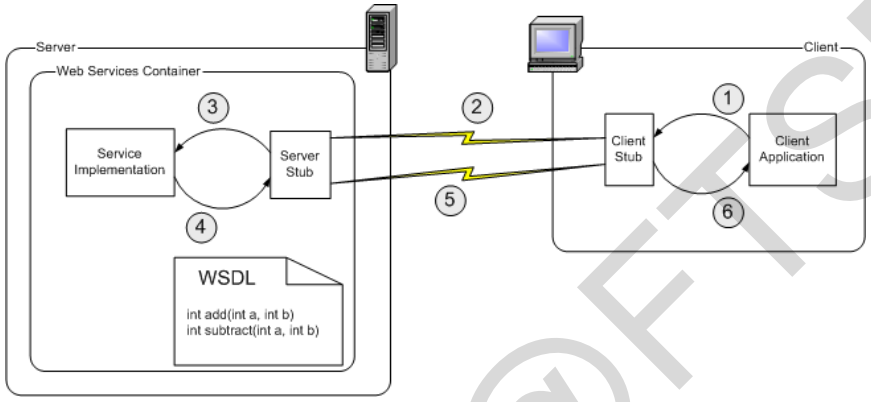



RAJAH 1. Komponen Perkhidmatan Web
(Sumber: IBM)

XML adalah format sejagat untuk data di web. XML membolehkan pembangun sistem menerangkan dengan mudah serta menghantar data yang berstruktur dan lengkap dari mana-mana aplikasi dalam cara yang konsisten, pantas dan standard (Gorgun 2004). Standard pemesejan (*messaging*) yang popular adalah SOAP. SOAP merupakan protokol berasaskan bahasa XML yang dapat digunakan untuk menganalisa permintaan dan respons pada perkhidmatan web sebelum dihantar ke rangkaian (Boezeman 2003). Komponen keselamatan (*security*) pula adalah terdiri dari pelbagai spesifikasi iaitu WS-Security, WS-Policy, WS-Privacy, WS-Trust, WS-Federation, WS-SecureConversation dan WS-Authorization. UDDI pula merupakan sebuah direktori yang membolehkan perkhidmatan perkhidmatan web ini dikesan dalam rangkaian (EngelBrecht 2009). WSDL adalah metadata yang merupakan sebuah bahasa

yang menggunakan XML untuk menerangkan kemampuan perkhidmatan web dan jenis perkhidmatan yang disediakan (Coetzee 2006).

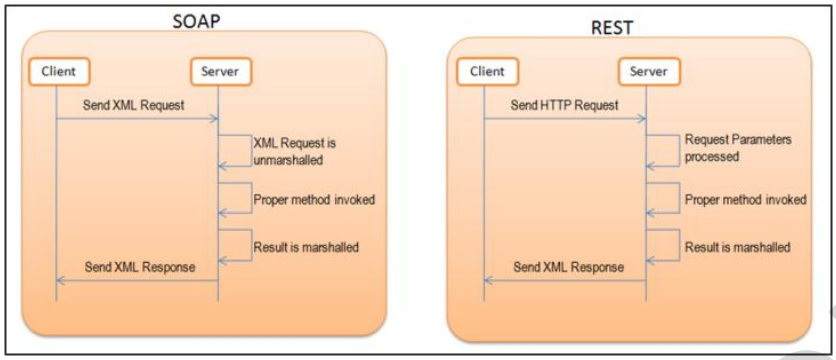
Oladosu et al (2009) menerangkan dengan teliti bagaimana perkhidmatan web berfungsi. Pada mulanya, pelanggan akan mengenalpasti lokasi perkhidmatan web yang memenuhi keperluan melalui UDDI. Kemudian, pelanggan akan mendapatkan keterangan WSDL bagi perkhidmatan web tersebut. Pelanggan kemudiannya menghasilkan stub dari perkhidmatan web dan memasukkannya ke dalam aplikasi. Rajah 2 memaparkan bagaimana teknologi perkhidmatan web digunakan oleh pelanggan dalam komunikasi dan pertukaran data.




RAJAH 2. Proses Menggunakan Perkhidmatan Web
(Sumber: Oladosu et al 2009)

1. Stub pelanggan (*client stub*) dipanggil setiap kali aplikasi pelanggan (*client application*) perlu menggunakan perkhidmatan web. Panggilan ini ditukar kepada permintaan SOAP, juga digelar proses penerbitan (*serializing*).
2. Permintaan SOAP dihantar melalui rangkaian dengan menggunakan protokol HTTP. Bekas perkhidmatan web (*web service container*) menerima permintaan SOAP tersebut dan menghantar kepada stub pelayan (*server stub*). Stub pelayan akan menukar permintaan SOAP ke dalam bentuk yang difahami oleh pelaksanaan perkhidmatan (proses *deserializing*).
3. Pelaksanaaan perkhidmatan (*service implementation*) menerima permintaan dari stub pelayan dan menjalankan tugas yang diminta.
4. Keputusan hasil operasi yang diminta diserah kepada stub pelayan yang akan mengubahnya kepada respons SOAP.
5. Respons SOAP dihantar melalui protokol HTTP kepada stub pelanggan. Stub pelanggan akan menukarnya ke dalam bentuk yang difahami oleh aplikasi pelanggan.
6. Akhirnya, aplikasi menerima hasil rujukan perkhidmatan web dan menggunakannya.

Selain SOAP, REST (*REpresentational State Transfer*) juga merupakan perkhidmatan web. Ia mula diperkenalkan oleh Roy Fielding (Mumbaikar & Padia 2013). Perkhidmatan web REST merupakan set antaramuka pengaturcaraan aplikasi (*application programming interface - API*) yang dibina di atas kerangka kerja RESTful bagi menjalankan operasi pelayan. Ia mempunyai fungsi yang sama seperti perkhidmatan web berprotokol SOAP tetapi REST menggunakan protokol HTTP untuk berinteraksi dengan pelayan. Rajah 3 memaparkan perbezaan antara REST dan SOAP.




RAJAH 3. Perbezaan Antara SOAP Dan REST
(Sumber: http://community.jaspersoft.com)

Berdasarkan kajian yang dilaksanakan oleh Mumbaikar & Padia (2013), prestasi perkhidmatan web REST adalah lebih baik berbanding perkhidmatan web SOAP kerana SOAP menghasilkan banyak trafik rangkaian mengakibatkan kependaman yang tinggi (*high latency*). Selain itu, REST menggunakan jalur lebar yang kurang kerana mesej tindakbalas yang bersaiz kecil (Wagh & Thool 2012).

## KAJIAN KESELAMATAN DALAM PERKHIDMATAN WEB

Keselamatan adalah sangat penting dalam dunia penjagaan kesihatan bagi memastikan integriti kandungan dan transaksi bagi memelihara kerahsiaan dan hak peribadi. Penggunaan perkhidmatan web dalam e-kesihatan melalui pelayar internet boleh membuka ruang kepada musuh bagi mencapai agenda yang tidak baik.

Terdapat pelbagai ancaman keselamatan terhadap penggunaan internet secara umum. Antaranya ialah akses tanpa kebenaran (*unauthorized access*), manipulasi parameter (*parameter manipulation*), penafian perkhidmatan (*denial of service*), mesej berulang (*message replay*) dan *network eavesdropping* (Teng & Ping). Model STRIDE telah diperkenalkan oleh Microsoft untuk menilai ancaman keselamatan. STRIDE merupakan akronim enam kategori ancaman iaitu, *spoofing* (perdayaan), *tampering* (pengacauan), *repudiation* (penafian), *information disclosure* (dedahan maklumat), *denial of service* (nafi khidmat) dan *elevation of privilege* (keistimewaan akses oleh yang tidak berhak). Jiang et al (2010), telah mengaplikasi model STRIDE ini bagi menilai keselamatan perkhidmatan web.

Bagi mencapai keselamatan maklumat, model yang sering digunapakai adalah CIA iaitu c*onfidentiality* (kerahsiaan), *integrity* (integriti) dan *availability* (kebolehsediaan). Selain itu, beberapa aspek penting lain dalam keselamatan maklumat adalah pengesahan, kebenaran dan tujuan bukan penafian (Holgersson 2005).

Kerahsiaan merujuk kepada tidak mendedahkan maklumat yang sensitif atau kritikal. Data harus dihantar dengan selamat. Ini termasuklah dengan menggunakan rangkaian yang selamat. Walau bagaimanapun, komunikasi yang melibatkan maklumat sensitif seperti nombor kad kredit, selalunya dilaksanakan penyulitan supaya jika maklumat tersebut jatuh ke tangan orang lain, ianya tidak dapat dibaca atau digunakan (Al-Hamdani 2010).

Integriti pula merujuk kepada jaminan bahawa tiada perubahan (penambahan atau pemadaman) pada maklumat, sama ada secara sengaja atau tidak. Maklumat tersebut boleh dihantar melalui rangkaian seperti dari pelayar web ke pelayan web, maklumat yang disimpan di

dalam pangkalan data atau sistem fail, atau maklumat yang dihantar dalam mesej perkhidmatan web dan diproses oleh orang tengah.

Kebolehsediaan adalah satu keadaan di mana sumber boleh diakses oleh pengguna yang sah dan dibenarkan pada bila-bila masa yang diperlukan.

Pengesahan (*Authentication*) merupakan satu proses bagi menentukan dakwaan identiti seseorang adalah sahih. Bentuk pengesahan yang paling biasa digunakan adalah kata laluan. Pengesahan boleh dilakukan berdasarkan satu atau lebih dari faktor-faktor berikut:

1. Sesuatu yang diketahui oleh pengguna, seperti kata laluan atau nombor pengenalan peribadi
2. Sesuatu yang dimiliki oleh pengguna, seperti kad ATM atau kunci
3. Suatu karakter fizikal pengguna, seperti cap jari atau corak retina atau karakter wajah.

Pengesahan adalah lebih kukuh jika dua atau lebih faktor digunakan (Gollman 2010).

Kebenaran (*Authorization*) adalah mekanisma yang mana ianya menentukan aras kebenaran kepada seseorang pengguna bagi mengawal keselamatan sumber. Ianya dapat mengelakkan dari penyalahgunaan sistem, aplikasi atau data selepas kebenaran telah diberi. Selalunya, kebenaran merujuk kepada proses yang menentukan apa yang boleh diakses oleh seseorang pengguna dan menyelenggara rekod-rekod terbabit. Penguatkuasaan kebenaran juga disebut sebagai kawalan akses.

Tujuan bukan penafian (*Non-repudiation*) adalah untuk memelihara pertanggungjawaban dan mengelakkan salah faham. Bukan penafian bermaksud apabila seseorang menghantar menghantar mesej, pada masa hadapan penghantar tidak boleh menafikan bahawa dia bertanggungjawab menghantar mesej itu. Bagi memastikan tiada dakwaan palsu, perlunya ada tandatangan digital yang mana ianya hanya boleh digunakan oleh penghantar yang sah dan mana-mana penerima boleh mengesahkannya.

## KAJIAN KESELAMATAN DALAM PERKHIDMATAN WEB DAN PENYELESAIAN SEDIA ADA

Perkhidmatan web sering digunakan dalam komunikasi antara aplikasi berbeza. Oleh kerana asas perkhidmatan web adalah XML, keselamatan perkhidmatan web perlu diintegrasi bersama keselamatan XML. Kajian yang dilaksanakan oleh Nakayama et al (2005) adalah melibatkan pelaksanaan keselamatan perkhidmatan web dengan menggunakan model industri pelancongan. Eksperimen yang telah dijalankan adalah menggunakan teknik penyulitan data XML dan tandatangan XML (*XML Signature*).

Sea dan Ng (2011) telah membuat kajian pelaksanaan penyulitan XML terhadap fail dengan menggunakan teknologi infrastruktur kunci awam (PKI). Fail tersebut termasuklah MP3, JPEG dan doc. Kaedah yang digunakan adalah dengan menjalankan operasi Base64Encoding terhadap data binari. Hasilnya digunakan untuk menjana sintaks XML berasaskan ASCII. Kemudian 16 bit kunci dijana sebagai kunci simmetri. Langkah seterusnya adalah untuk menyulitkan kunci penyulitan dengan kunci awam pengguna menggunakan algoritma kunci asimetri. Mereka telah melaksanakan penyulitan XML dan menggunapakai PKI yang mematuhi draf kerja W3C bagi memastikan keselamatan XML.

Menurut Nithin dan Anupkumar (2012), mereka telah mencadangkan satu algoritma baru iaitu XBMRSA (*XML Batch Multi-Prime RSA*) untuk menyulitkan dokumen XML. Kajian yang dilaksanakan membandingkan antara RSA standard dan XBMRSA menunjukkan penggunaan masa pengkomputeran yang lebih pantas dan saiz yang lebih kecil berbanding RSA konvensional.

Kajian yang dibuat oleh Mukherjee et al (2013), mereka menyenaraikan protokol yang dapat menjamin keselamatan perkhidmatan web. Antara yang dinyatakan adalah Security

Assertion Markup Language (SAML), XML Encryption dan tandatangan XML. Walau bagaimanapun, terdapat impak dari segi masa kerana beban berlebihan algoritma dan sijil yang digunakan dalam kaedah ini. Jadual 1 memaparkan rumusan kajian keselamatan dan penyelesaian sedia ada.

JADUAL 1. Kajian Keselamatan Dan Penyelesaian

| Pengkaji | Komponen kajian | Penyelesaian | Tahun |
|---|---|---|---|
| Kojiro et al | Pelaksanaan keselamatan perkhidmatan web dengan model industri pelancongan | Penyulitan XML dan tandatangan XML | 2005 |
| Sea dan Ng | Pelaksanaan keselamatan terhadap aliran dan pertukaran data berasaskan fail | Penyulitan XML | 2011 |
| Nithin dan Anupkumar | Kajian perbandingan antara RSA standard dan XBMRSA untuk menyulitkan dokumen XML | Mencadangkan algoritma baru iaitu XBMRSA (*XML Batch Multi-Prime RSA*) untuk menyulitkan dokumen XML | 2012 |
| Sudeep dan Rizwan | Penyenaraian spesifikasi keselamatan perkhidmatan web | SAML, penyulitan XML dan tandatangan XML | 2013 |

## KESELAMATAN MENGGUNAKAN KAEDAH PELBAGAI LAPISAN KOMUNIKASI

Penggunaan satu jenis algoritma penyulitan dalam komunikasi adalah kurang fleksibel kerana keperluan komunikasi adalah berbeza dalam sesuatu organisasi. Sekiranya organisasi memerlukan keperluan keselamatan yang berbeza, teknologi sekarang tidak dapat menyediakan kemudahan tersebut. Sebagai contoh, jika organisasi tersebut perlu menukar kekuatan keselamatan (*security strength*) SSL, ia tidak boleh disediakan secara fleksibel.

Rossilawati et al (2011) telah memperkenalkan kaedah pelbagai lapisan komunikasi, untuk keselamatan komunikasi e-kesihatan dengan menggunakan teknik multiagen. Lapisan keselamatan adalah diklasifikasikan mengikut tahap keselamatan dalam komunikasi tersebut. Jadual 2 memaparkan panjang kunci yang dicadangkan berdasarkan jenis komunikasi.

JADUAL 2. Panjang Kunci Berdasarkan Jenis Komunikasi
(Sumber: Rossilawati 2010)

| Komunikasi pelbagai lapisan | Panjang kunci (dalam bit) |
|---|---|
| Lapisan 1 (Rahsia besar) | 193 dan ke atas |
| Lapisan 2 (Kerahsiaan yang tinggi) | 129 hingga 192 |
| Lapisan 3 (Proprietari) | 112 hingga 128 |
| Lapisan 4 (Kegunaan dalaman sahaja) | 80 hingga 111 |

Sebagai contoh, dalam e-kesihatan, terdapat pelbagai pengguna yang berkomunikasi antara satu sama lain, yang berkongsi pelbagai jenis maklumat. Tahap sensitiviti keselamatan yang diperlukan juga adalah berbeza-beza. Sebagai contoh, maklumat yang disampaikan oleh doktor kepada jururawat lebih tinggi tahap sensitif daripada maklumat yang dikongsi antara doktor dan pekerja sosial. Sekiranya organisasi perlu menguruskan jenis maklumat yang berbeza-beza, teknologi sedia ada tidak menyediakan kefleksibelan keselamatan.

## E-KESIHATAN DAN PERKHIDMATAN WEB

Menurut World Health Organization (WHO), e-kesihatan merupakan penggunaan informasi dan teknologi komunikasi untuk kesihatan. Ini termasuklah merawat pesakit, menjalankan kajian, mendidik tenaga kerja di bidang kesihatan, mengesan penyakit dan memantau kesihatan orang

awam. Fokus utama sistem penjagaan kesihatan awam adalah untuk menyediakan penjagaan perubatan yang berkualiti tinggi pada kos yang terhad di samping mematuhi hak asasi seseorang pesakit. Beberapa kajian telah dilaksanakan terhadap aplikasi e-kesihatan yang digunakan di beberapa buah negara.

Isu keselamatan dalam e-kesihatan juga mendapat perhatian dari para pengkaji. Kajian oleh Rossilawati et al (2008) telah memperkenalkan model keselamatan dengan pendekatan pelbagai lapisan keselamatan dalam komunikasi di bidang kesihatan. Mereka mengklasifikasikan data dengan 5 tahap sensitiviti iaitu dari tahap sangat sensitif, tinggi sensitif, sederhana sensitif, kurang sensitif kepada tidak sensitif dan menggunakan teknik kriptografi yang berbeza bagi setiap tahap. Sun et al (2011) turut bersetuju bahawa kerahsiaan maklumat dalam e-kesihatan adalah penting. Mereka mencadangkan Healthcare System for Patient Privacy (HCPP) berasaskan kriptografi dan infrastruktur rangkaian wayarles sedia ada terhadap Electronic Health Record (EHR). Manakala Benaloh et al (2009) pula mencadangkan cabaran terhadap privasi pesakit dapat diatasi dengan menguatkuasaan 2 aspek iaitu melalui teknik penyulitan dan hak akses (*access right*).

Menurut Della et al (2005), projek Artemis menggunakan perkhidmatan web untuk pertukaran maklumat dalam bidang penjagaan kesihatan. Projek ini membangunkan perkhidmatan web semantik berasaskan rangka kerja interoperabiliti bagi domain kesihatan. Contohnya, apabila pengguna mencari perkhidmatan untuk mendaftarkan pesakit ke hospital, beliau seharusnya mendapatkan perkhidmatan tersebut berdasarkan maksudnya tanpa bergantung kepada bahasa perkhidmatan itu dipanggil.

Selain itu, kajian yang dilaksanakan oleh Helmer et al (2011) terhadap 48 produk rekod kesihatan peribadi pihak ketiga yang berasaskan web menunjukkan peratusan penggunaan perkhidmatan web sebanyak 6.25% bagi mekanisma pertukaran data. Sebagai contoh adalah perkhidmatan yang menyediakan antaramuka pengaturcaraan untuk mengira risiko serangan jantung dengan data dari rekod kesihatan peribadi.

## JURANG KAJIAN

Penggunaan satu jenis algoritma penyulitan dalam komunikasi adalah tidak fleksibel kerana tahap sensitiviti data adalah berbeza dari pelbagai lapisan komunikasi. Kajian oleh Rossilawati et al (2011) memperkenalkan model komunikasi pelbagai lapisan untuk keselamatan komunikasi e-kesihatan dengan menggunakan teknik multiagen. Kajian ini akan fokus kepada keselamatan perkhidmatan web dalam pelbagai lapisan komunikasi dengan penggunaan panjang kunci *(key length)* kriptografi berbeza berdasarkan tahap sensitiviti maklumat dalam bidang e-kesihatan.

Terdapat pelbagai jenis lapisan komunikasi yang terlibat dalam e-kesihatan. Tahap sentiviti keselamatan yang diperlukan juga adalah berbeza-beza. Maklumat yang disampaikan oleh doktor kepada jururawat lebih tinggi tahap sensitif daripada maklumat yang dikongsi antara doktor dan pekerja sosial. Oleh yang demikian, justifikasi kajian ini adalah kerana kekangan teknologi sedia ada menyediakan pelbagai lapisan keselamatan mengikut keperluan.

## METOD

Bagi membangunkan sistem, keperluan sistem dan perisian yang akan digunakan ditentukan terlebih dahulu. Pemilihan telah dibuat bagi kajian ini dengan menggunakan perisian Eclipse, bahasa pengaturcaraan Java, pangkalan data MySQL dan pelayan web Apache Tomcat 7.0.

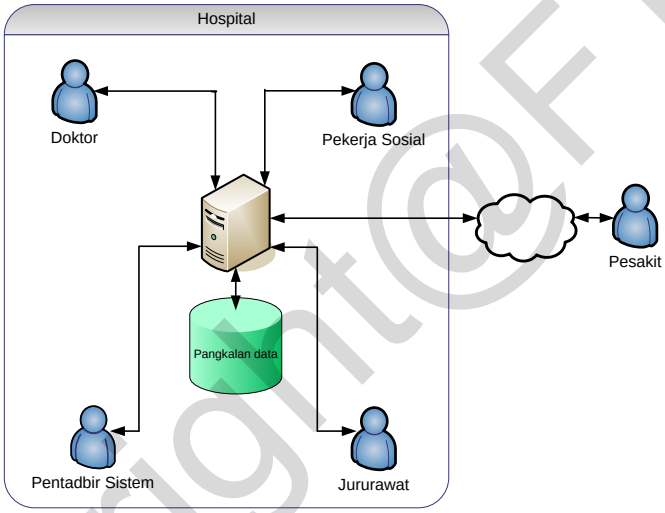
SENARIO SISTEM

Berdasarkan kajian oleh Rossilawati (2010), keselamatan pelbagai lapisan terbahagi kepada 5 peringkat seperti dalam Jadual 3 di bawah.

JADUAL 3. Pelbagai Lapisan Keselamatan
(Sumber: Rossilawati 2010)

| | |
|---|---|
| Lapisan 1 | Rahsia Besar (*Top secret*) |
| Lapisan 2 | Kerahsiaan yang tinggi (*Highly confidential*) |
| Lapisan 3 | Proprietari (*Proprietary*) |
| Lapisan 4 | Kegunaan dalaman sahaja (*Internal use only* ) |
| Lapisan 5 | Awam (*Public*) |

Rajah 4 memaparkan persekitaran e-kesihatan yang akan digunakan dalam kajian ini. Kajian ini melibatkan 5 aktor iaitu Doktor, Jururawat, Pesakit, Pekerja Sosial dan Pentadbir Sistem. Setiap aktor memainkan peranan masing-masing.




RAJAH 4. Persekitaran E-kesihatan

Urutan peristiwa dimulai dengan kedatangan pesakit ke hospital untuk melakukan pemeriksaan kesihatan.

1. Jururawat akan mendaftarkan maklumat peribadi pesakit ke dalam pangkalan data.
2. Doktor yang membuat pemeriksaan akan mengisi maklumat pemeriksaan, hasil diagnosis dan cadangan ke atas pesakit ke dalam sistem.
3. Pesakit yang didiagnos dan perlu dimasukkan ke wad kemudiannya dimasukkan butir perincian seperti nombor wad dan nombor katil ke dalam sistem oleh jururawat.
4. Pekerja sosial yang datang akan memeriksa jadual harian bagi pesakit di bawah seliaannya bagi mendapatkan maklumat peribadi dan nombor wad.
5. Pesakit yang telah dibenarkan keluar oleh pihak hospital boleh mendapatkan khidmat rundingan dengan doktor melalui sistem.
6. Pesakit juga boleh membuat temujanji dengan pekerja sosial bagi mengadakan sesi kaunseling.
7. Pentadbir sistem berfungsi untuk menyelenggara maklumat akaun pengguna sistem dan bertanggungjawab melaksanakan hebahan melalui sistem kepada pengguna yang terlibat.

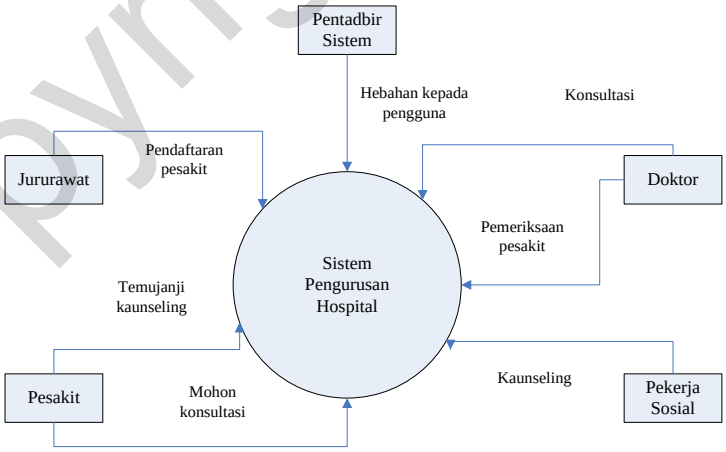
Berikut merupakan peringkat data kritikal dari senario di atas (Jadual 4) serta penggunaan panjang kunci algoritma yang akan digunakan bagi penyulitan data.

JADUAL 4. Data Kritikal Dan Penggunaan Panjang Kunci Penyulitan

| Komunikasi | Data kritikal | Tahap | Algoritma |
|---|---|---|---|
| Komunikasi antara doktor dan jururawat | Doktor membincangkan maklumat penyakit dan ubat yang perlu | sangat sensitif | AES 256 + SSL |
| Komunikasi antara doktor dan pesakit | Doktor membincangkan maklumat penyakit dan memberi khidmat rundingan kepada pesakit | sangat sensitif | AES 256 + SSL |
| Komunikasi antara jururawat dan pesakit | Jururawat membincangkan maklumat ubat yang perlu diambil oleh pesakit | sangat sensitif | AES 256 + SSL |
| Komunikasi antara jururawat dan pekerja sosial | Jururawat memaklumkan maklumat awam pesakit dan maklumat wad pesakit | sederhana sensitif | AES 192 |
| Komunikasi antara pesakit dan pekerja sosial | Pesakit membuat temujanji bagi sesi kaunseling dengan pekerja social | sensitif | AES 128 |
| Komunikasi antara pentadbir sistem dan doktor, jururawat dan pekerja social | Pentadbir sistem bertanggungjawab membuat hebahan berkaitan hospital kepada kakitangan lain | kurang sensitif | SSL |

## REKABENTUK DAN PEMBANGUNAN

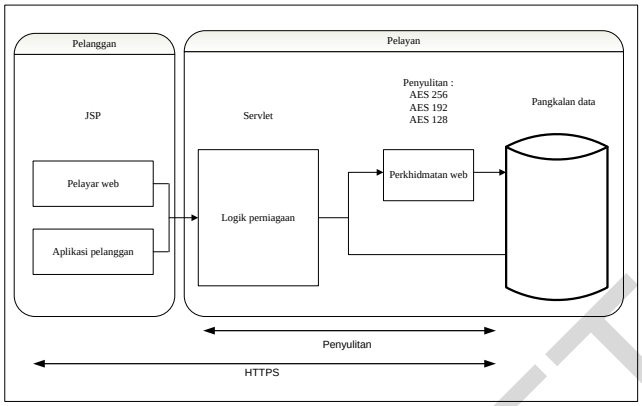
Rajah 5 menunjukkan gambar rajah konteks bagi sistem yang dibangunkan. Sistem Pengurusan Hospital ini mempunyai lima jenis pengguna beserta peranan masing-masing. Pentadbir sistem bertanggungjawab untuk membuat hebahan maklumat berkaitan hospital kepada pengguna sistem. Jururawat pula bertanggungjawab bagi mendaftarkan maklumat pesakit ke dalam sistem ini. Doktor akan mengemaskini maklumat kesihatan pesakit hasil pemeriksaan yang telah dijalankan. Doktor juga akan memberi konsultasi kepada pesakit melalui sistem ini. Pesakit boleh membuat temujanji dengan pekerja sosial untuk mengadakan sesi kaunseling. Jika perlu, pesakit boleh membuat pertanyaan bagi kendapatkan khidmat rundingan daripada doktor. Manakala pekerja sosial berperanan untuk memberi maklumbalas berkaitan permohonan pesakit untuk menjalankan sesi kaunseling.




RAJAH 5. Gambar Rajah Aliran Data

Berdasarkan analisa keperluan dan pangkalan data yang telah dibuat, satu sistem perkhidmatan web yang menggunakan kaedah penyulitan telah dibangunkan. Rajah 6 memaparkan senibina keselamatan yang digunakan dalam pembangunan sistem ini. Kaedah

penyulitan dilaksanakan bagi tiga jenis panjang kunci AES iaitu 256 bit bagi data paling sensitif, 192 bit bagi data sederhana sensitif dan 128 bit bagi data kurang sensitif. Bagi melaksanakan fungsi kriptografi dalam Java, kajian ini bergantung kepada Java Cryptography Extension (JCE). JCE boleh dimuaturun melalui http://www.oracle.com/technetwork/java/javase/downloads.




RAJAH 6. Senibina Keselamatan

## ANALISIS DAN KEPUTUSAN

Objektif eksperimen adalah untuk memerhatikan dan menilai prestasi keselamatan bagi setiap lapisan dalam keselamatan pelbagai lapisan dengan membuat perbandingan bagi masa komunikasi berlangsung di antara perkhidmatan web dengan atau tanpa penyulitan. Kami juga menilai kecekapan tanpa penyulitan yang memindahkan teks biasa tanpa mekanisma keselamatan bagi mengukur kos overhed keselamatan.

### PENYEDIAAN EKSPERIMEN

Persekitaran dikawal hanya menggunakan sebuah komputer. Eksperimen dijalankan dengan menggunakan 4 jenis saiz teks biasa berbeza iaitu 1KB, 3KB, 5KB dan 7KB. Eksperimen ini direka supaya merangkumi mekanisma keselamatan data dan keselamatan saluran.

JADUAL 5. Persediaan Eksperimen

| Lapisan | Mekanisma keselamatan | Algoritma |
|---|---|---|
| Lapisan 1 | Keselamatan data dan saluran SSL | AES 256 + SSL |
| Lapisan 2 | Keselamatan data dan saluran SSL | AES 192 |
| Lapisan 3 | Keselamatan data dan saluran SSL | AES 128 |
| Lapisan 4 | Keselamatan saluran SSL | SSL |
| Lapisan 5 | Tiada keselamatan | - |

Sebagaimana yang dipaparkan dalam Jadual 5, empat penetapan keselamatan digunakan. Pada Lapisan 1, AES 256 bit dan SSL digunakan bagi keselamatan data keselamatan saluran SSL. Manakala bagi Lapisan kedua pula menggunakan AES 192 bit . Manakala bagi Lapisan ketiga menggunakan AES 128 bit. Lapisan keempat pula hanya menggunakan SSL sebagai keselamatan saluran. Lapisan terakhir iaitu Lapisan kelima tidak menggunakan mekanisma keselamatan bagi mewujudkan perbezaan lapisan. Keselamatan SSL disediakan secara automatik dengan penetapan pada konfigurasi Apache Tomcat.

### PENGUKURAN MASA

Kaedah pengukuran yang digunakan adalah *System.currentTimeMillis()*, yang mana ia mengembalikan masa dalam milisaat. Pengiraan selang masa adalah antara penghantaran dan penerimaan. Walau bagaimanapun, nilai ini mungkin berubah bergantung kepada spesifikasi komputer yang digunakan. Dalam eksperimen ini, masa yang digunakan adalah masa purata. Kami melaksanakan ujian sebanyak 30 kali bagi setiap parameter (*n=30*). Kesemua hasil eksperimen mengikut parameter dicampur dan kemudian dibahagi dengan nilai 30 bagi mendapatkan nilai purata. Nilai 30 diambil supaya kami boleh mendapatkan bacaan masa yang konsisten.

## KEPUTUSAN EKSPERIMEN

Bagi eksperimen yang telah dijalankan, kami menilai masa bagi pelaksanaan berikut:

1. Masa pemprosesan, iaitu masa penjanaan teks sifer
2. Masa pemprosesan penghantaran teks
3. Overhed keselamatan

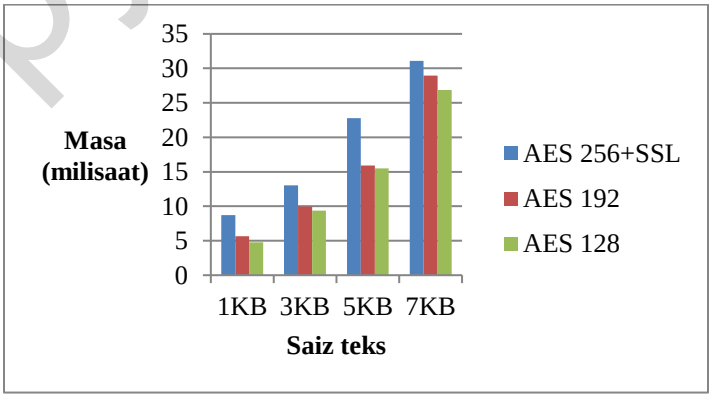
*Masa pemprosesan*

Seperti yang diterangkan sebelum ini, masa pemprosesan adalah masa yang diambil bagi menjana teks sifer. Jadual 6 memaparkan masa yang diambil untuk penjanaan teks sifer.

JADUAL 6. Pengukuran Masa Untuk Penjanaan Teks Sifer

| Mekanisma keselamatan | 1KB | 3KB | 5KB | 7KB |
|---|---|---|---|---|
| AES 256+SSL | 8.73 | 13.03 | 22.76 | 31.10 |
| AES 192 | 5.63 | 9.97 | 15.93 | 28.97 |
| AES 128 | 4.77 | 9.37 | 15.47 | 26.87 |

Berdasarkan jadual di atas, masa penyulitan bertambah seiring dengan peningkatan saiz teks. Keputusan juga menunjukkan AES 128 bit adalah lebih cepat berbanding AES 192 bit dan AES 256 bit. Hasil penemuan ini, kepanjangan kunci yang pendek mempunyai masa penyulitan yang lebih pantas berbanding kunci yang panjang bagi kesemua teks biasa bagi algoritma AES. Rajah 7 memaparkan graf hasil pengukuran masa yang diambil bagi menjana teks sifer.



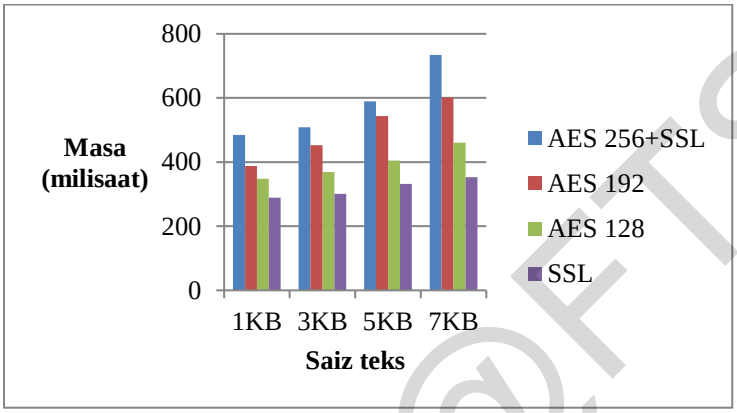

RAJAH 7. Graf Masa Penjanaan Teks Sifer

*Masa pemprosesan penghantaran teks*

Jadual 7 dan Rajah 8 memaparkan jumlah masa bagi penghantaran teks dengan penyulitan. Manakala Jadual 8 dan Rajah 9 memaparkan jumlah masa penghantaran teks tanpa penyulitan.

JADUAL 7. Pengukuran Masa Untuk Penghantaran Teks Dengan Penyulitan

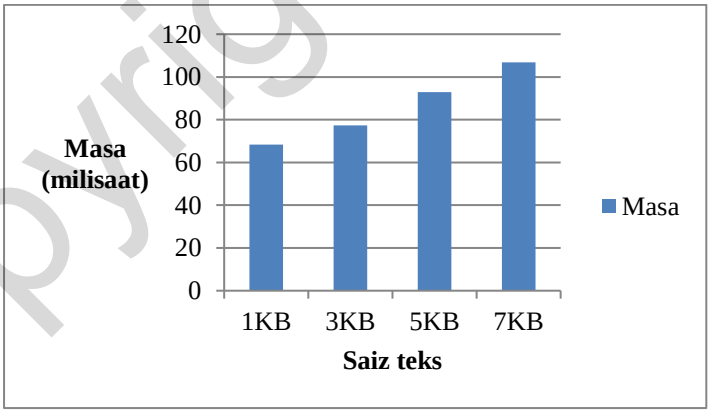
| Mekanisma keselamatan | 1KB | 3KB | 5KB | 7KB |
|---|---|---|---|---|
| AES 256+SSL | 484.73 | 508.67 | 589.37 | 734.30 |
| AES 192 | 388.20 | 452.50 | 543.73 | 601.60 |
| AES 128 | 348.00 | 369.30 | 405.10 | 461.03 |
| SSL | 289.34 | 301.20 | 331.67 | 353.30 |




RAJAH 8. Graf Masa Penghantaran Teks Dengan Penyulitan

JADUAL 8. Pengukuran Masa Untuk Penghantaran Teks Tanpa Penyulitan

| Saiz teks | 1KB | 3KB | 5KB | 7KB |
|---|---|---|---|---|
| Masa | 68.40 | 77.33 | 92.93 | 106.80 |




RAJAH 9. Graf Masa Pemprosesan Penghantaran Teks

*Overhed Keselamatan*

Kos keselamatan overhed merupakan masa tambahan yang diambil bagi membolehkan ciri keselamatan diaplikasikan ke dalam komunikasi iaitu fungsi penyulitan. Pengiraan bagi kos overhed adalah perbezaan masa perkhidmatan web dengan penyulitan dan perkhidmatan web tanpa penyulitan. Perbandingan dibuat dengan menggunakan parameter 7KB teks pada kedua-

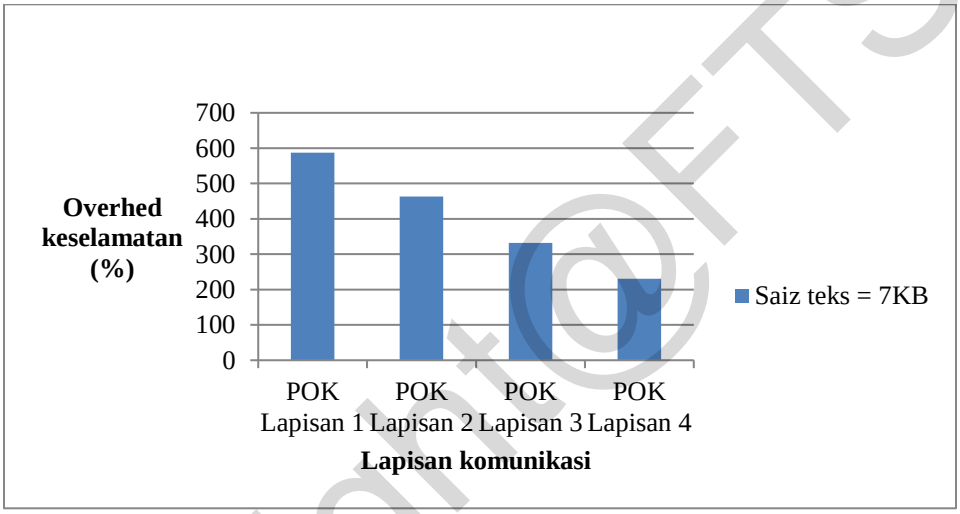
dua jenis sistem. Peratusan overhed keselamatan (POK) diukur dengan menggunakan formula berikut:

$$POK = ((TransaksiEn - TransaksiNen) / TransaksiNen) * 100,$$

di mana *TransaksiEn* adalah masa penghantaran teks bagi Lapisan n dengan mekanisma keselamatan, dan *TransaksiNen* merupakan masa penghantaran teks tanpa mekanisma keselamatan. Hasil eksperimen dipaparkan dalam Jadual 9 dan Rajah 10.

JADUAL 9. Peratusan Overhed Keselamatan

| Saiz fail | 1KB |
|---|---|
| POK Lapisan 1 | 587.55% |
| POK Lapisan 2 | 463.30% |
| POK Lapisan 3 | 331.68% |
| POK Lapisan 4 | 230.81% |




RAJAH 10. Graf Peratusan Overhed Keselamatan

Jadual 9 memaparkan overhed keselamatan bagi penggunaan penyulitan. Keputusan menunjukkan komunikasi Lapisan 1 mempunyai overhed yang paling tinggi iaitu 587.55% berbanding sistem tanpa penyulitan. Layer 1, iaitu lapisan yang mengaplikasikan mekanisma penyulitan AES 256 bit mempunyai overhed paling tinggi berbanding lapisan lain. Manakala lapisan keempat iaitu mekanisma SSL mempunyai overhed paling rendah iaitu 230.81%.

## PERBINCANGAN DAN PENILAIAN

Hasil penilaian prestasi keselamatan yang telah dijalankan membawa kepada kesimpulan berikut:

1. Penjanaan teks sifer lebih cepat dengan menggunakan panjang kunci yang lebih pendek.
2. Masa pemprosesan keseluruhan di bahagian penghantar di Lapisan 1 lebih lambat apabila kedua-dua keselamatan data dan keselamatan saluran digunakan.
3. Lapisan 1 dengan membawa saiz teks yang paling besar menggunakan masa pemprosesan yang paling lama disebabkan overhed keselamatan saluran.
4. Lapisan 4 dengan keselamatan saluran sahaja (SSL) mempunyai prestasi yang hampir sama dengan prestasi keselamatan data melalui mekanisma penyulitan.
5. Pertambahan saiz teks mengakibatkan pertambahan masa pemprosesan bagi setiap lapisan keselamatan.

6. Kesimpulan keseluruhan, sistem perkhidmatan web dengan penyulitan adalah lebih lambat berbanding sistem perkhidmatan web tanpa penyulitan.

## KESIMPULAN

Kajian ini telah menilai kepentingan keselamatan maklumat khususnya dalam bidang kesihatan. Komunikasi dan pertukaran maklumat di antara pihak yang berkepentingan perlu dilindungi kerana maklumat sensitif yang terlibat. Kajian ini pula menekankan tentang penggunaan perkhidmatan web sebagai perantara untuk pertukaran maklumat tersebut.

Dengan mengaplikasikan mekanisma keselamatan seperti yang telah diterangkan di atas, keputusan ujian mendapati bahawa semakin besar saiz teks, semakin tinggi jumlah masa pemprosesan. Begitu juga dengan masa penjanaan teks sifer juga turut bertambah. Penggunaan keselamatan saluran iaitu SSL turut mempengaruhi hasil ujian. Sistem perkhidmatan web dengan penyulitan adalah lebih lambat berbanding sistem perkhidmatan web tanpa penyulitan. Kesimpulannya, aplikasi ciri keselamatan ke atas perkhidmatan web perlu ditoleransi dengan pemprosesan masa yang lebih perlahan.

## CADANGAN KAJIAN LANJUTAN

1. Kajian ini hanya meliputi skop proses penyulitan perkhidmatan web. Oleh itu, berikut dicadangkan skop lain bagi kajian lanjutan:
2. Sokongan bagi perkhidmatan selain dari pertukaran maklumat dalam bentuk teks biasa.
3. Menambahbaik protokol keselamatan dengan mengambilkira keperluan tandatangan digital dan fungsi hash.

## PENUTUP

Perkhidmatan dalam talian menjadi perkara penting dalam kehidupan seharian. Oleh itu, ancaman keselamatan semasa melayari perkhidmatan dalam talian perlu ditangani. Keselamatan adalah penting bagi pertukaran maklumat khususnya di bidang kesihatan. Aplikasi kriptografi khasnya kaedah penyulitan dalam program merupakan salah satu langkah dalam memastikan kerahsiaan maklumat terpelihara.

## RUJUKAN

Al-Hamdani, W.A. 2010. XML Security in Healthcare Web Systems. *Journal ACM 978-1-60558-661-8/10/10*

Anshari, M., Almunawar, M. N., Low, P. K. C. & Wintz, Z. 2012. Customer Empowerment in Healthcare Organisations Through CRM 2.0: Survey Results from Brunei Tracking a Future Path in E-Health Research. *ASEAS – Austrian Journal of South-East Asian Studies, 5(1), 139-151.*

Baroud, B.M. 2008. How Ready Are the Stakeholders in the Palestinian HealthCare System in the Gaza Strip to Adopt E-Health?. University of Calgary.

Benaloh, J., Chase, M., Horvitz, E. & Lauter, K. 2009. Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. *Journal ACM 978-1-60558-784-4/09/11*

Boezeman, R. J. 2003. Web Services Security. Master's thesis Computing Science, University of Nijmegen Software Engineering, Programme of the Oxford University Computing Laboratory University of Oxford.

Brekken, L.A. & Asprang, R.F. 2006. Adding Security to Web Services, An Automatic, Verifiable, and Centralized Mechanism for Web Services Input Validation. Master of Science in Communication Technology, Department of Telematics Norwegian University of Science and Technology.

Chen, M., Chen, N.K. & Shao, B.M. 2003 The Implications and Impacts of Web Services to Electronic Commerce Research and Practices. *Journal of Electronic Commerce Research, Vol. 4, No. 4.*

Coetzee, M. 2006. WSACT – A Model for Web Services Access Control incorporating Trust. Doctor of Philosophy Computer Science Faculty of Engineering, Built Environment and Information Technology at the University of Pretoria.

Della, V. E., Cerizza, D., Bicer, V., Kabak, Y., Laleci, G. & Lausen, H. 2005. The Need for Semantic Web Service in the eHealth. W3C workshop on Frameworks for Semantics in Web Services, 2005.

EngelBrecht, M.G. 2009. A Service-Oriented Grid Environment with On-Demand QoS Support. Doctor Dissertation University of Wien.

Gollmann, D. 2010. Computer Security. John Wiley & Sons, 2nd edition.

Gorgun, I. 2004. Deploying and Invoking Secure Web Services over JXTA Framework. Master of Science in Computer Engineering. The Graduate School of Natural and Applied Sciences of Middle East Technical University.

Helmer, A., Lipprandt, M., Frenken, T., Eichelberg, M & Hein, A. 2011. Empowering Patients through Personal Health Records: A Survey of Existing Third-Party Web-Based PHR Products. *Electronic Journal of Health Informatics, 2011; Vol 6(3): e26.*

Holgersson , J. & Söderström, E. 2005. Web Service Security – Vulnerabilities and Threats within the Context ff WS-Security. Report of Standards and Innovation in Information Technology (SIIT) 2005. September 21-23, 2005.

Jiang, L., Chen, H. & Deng, F. 2010. A Security Evaluation Method Based on STRIDE Model for Web Service. *Journal IEEE 978-1-4244-5874-5/10.*

Mukherjee, Sudeep, Dr. Rizwan Beg, Srivastava, Amit & Khan, Riyazuddin. 2013. Overview of Secured Web Services Specifications. *Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).*

Mumbaikar, Snehal & Padiya, Puja. 2013. Web Services Based On SOAP and REST Principles. *International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153* .

Nakayama, K., Ishizaki, T. & Oba, M. 2005. Application of Web Security Using Travel Industry Model. *Proceedings of the The 2005 Symposium on Applications and the Internet Workshops (SAINT-W'05).*

Nithin N & Anupkumar M Bongale. 2012. XBMRSA: A New XML Encryption Algorithm. *2012 World Congress on Information and Communication Technologies.*

Oladosu, J.B., Ajala, F.A. & Popoola, O.O. 2009 On The Use of Web Services Technology in E-Health Applications. *Journal of Theoretical and Applied Information Technology*.

Rossilawati Sulaiman, Sharma, Dharmendra, Ma, Wanli & Tran, D. 2008. A Security Architecture for e-Health Services. *2008 International Conference on Advanced Communications Technology.*

Rossilawati Sulaiman. 2010. MAgSeM: A Multi-agent based Security Model for Secure Cyber Services. PhD Thesis, The Faculty of Information Sciences and Engineering. University of Canberra ACT 2601 Australia.

Rossilawati Sulaiman, Sharma, Dharmendra, Ma, Wanli & Tran, D. 2011. A New Security Model using Multilayer Approach for E-Health Services. *Journal of Computer Science 7 (11): 1691-1703, 2011.*

Sea, Chong Seak & Ng, Kang Siong. 2011. A File-based Implementation of XML Encryption. *2011 5th Malaysian Conference in Software Engineering (MySEC).*

Sun, J., Zhu, X., Zhang, C. & Fang, Y. 2011. HCCP: Cryptography Based Secure HER System for Patient Privacy and Emergency Healthcare. *2011 31st International Conference on Distributed Computing Systems.*

Wagh, Kishor & Thool, Ravindra. 2012. A Comparative Study of SOAP Vs REST Web Services ProvisioningTechniques for Mobile Host. Journal of Information Engineering and Applications Vol 2, No.5, 2012