AN ENHANCED TRIPLE DATA ENCRYPTION STANDARD (TDES) ALGORITHM TO SECURE HEALTH LEVEL SEVEN (HL7) DATA TRANSFER

Michael Tetteh Asare[1], Yaw Marfo Missah[2]

[1]Michael Tetteh Asare Department of Information Technology Valley View University Accra, Ghana
[2]Yaw Marfo Missah Department of Computer Kwame Nkrumah University of Science and Technology Kumasi, Ghana

---***---

Abstract - *The confidentiality of patient information is very important; this is because it contributes to the efficiency of healthcare delivery. The willingness of patients to disclose their information is based on the trust that their information is kept secret.*

This study looked at a way to enhance Triple Data Encryption Algorithm (TDES/TDEA) to secure HL7 message or data on transit. The study looked at encrypting the encoded and validated HL7 message before transmission; the message was encoded and encrypted. Upon arrival at its destination, the message was decrypted and decoded thereby securing patients' data. The findings of the research show that, in order for any information sent through an HL7 Messaging System to be secured, to facilitate hospital–patient trust and confidentiality, there is the need for an Enhanced Triple Data Encryption Algorithm (ETDES).

Keywords

HL7, ETDES, Algorithm, Cipher, Decipher, Cryptography, Encryption, Decryption

1. Introduction

Due to the increasing need to understand hospital-patient and even workers of health facilities status and behavioural patterns, hospitals amass a great deal of confidential information about their employees, patients, medical products, research and financial status. Most of these information are collected, processed, stored on computers, then transmitted across networks to other computers (1).

It has also been realized that, management of healthcare information in relation to time and cost is very important since human lives are at stake. A lot of clinical applications are now in existence that operates within individual healthcare institutions; there is the need for some kind of interoperability or common level of information system that manages healthcare information across the nation.

Though many of these institutions are aspiring to achieve this goal, it has been realized that, many of their systems are incompatible (2). Furthermore, securing data during transmission across networks is another major concern to be considered to ensure the realization of this kind of common platform in the nation.

According to Mweebo (3), patients' privacy is paramount because any disclosure of personal health information such as the HIV status of the patient may result in stigmatization, unemployment, and denial of medical benefits. In addition, patients are likely to suffer financial losses from illegal transfer of finances if billing information is accessed by unauthorised staff.
Vithiatharan, (4) indicated that, although attempts are being made to hide medical data, it does not guarantee its full protection.
In the case of Ghana, when a patient is being transferred from one hospital to the other, a transfer form will have to be completed by the medical officers initiating the transfer. This will include medical records like the patients history, current condition, drugs administered, observation made, just to mention a few. Since this is a human institution, the tendency to introduce error is very likely or high. This process will take a lot of time; if this is an emergency situation, casualties may be recorded. What if there is a system that allows the medical records of the patient to be pulled or accessed seamlessly, from the hospital information system of another hospital with the use of

their health insurance number? In order to achieve this, Health Level Seven (HL7) will have to be implemented.

HL7 refers to a set of international standards for the transfer of administrative and clinical data between software/web applications used by a variety of hospitals and healthcare providers (5). It was founded in 1987 (5) and has a number of benefits:

- It facilitates the seamless exchange of data between health and medical institutions.
- Health providers can use HL7 interface engine to achieve the benefits that come with current legacy systems (Information Systems) without any major investment in new technologies; this lowers cost and extends the life and efficiencies of existing systems.
- There is also an opportunity to connect with systems outside the healthcare provider, which include providers of outsourced services like radiology (6).

However, there are few problems with the HL7. Although it makes it possible for seamless data exchange, data being transferred over a network is not safe and can easily be intercepted and read by anybody with little knowledge about HL7 standards (7)

2. Related Work

Triple Data Encryption Standard Algorithm

Triple DES in cryptography is refered to as Symetric Block Cipher, It applies Data Encryption Standard Cipher Algorithm three times to each block of data (8). The TDES process is made up of the following steps: the user generates and distributes a 3TDES key K, which is made up of three different DES keys K1, K2 and K3. This implies that the actual 3TDES key has length 3×56 = 168 bits (9). The encryption scheme is shown belows:

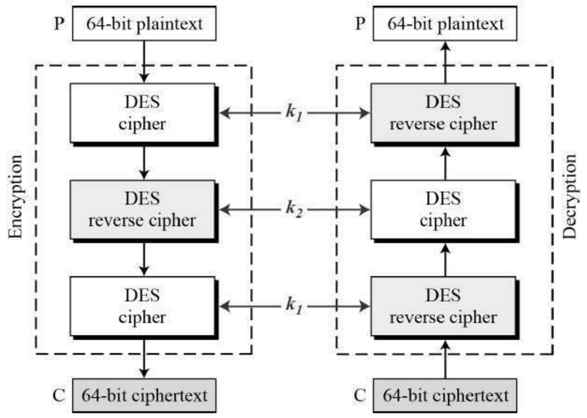


Figure 1. Encryption and decryption process of TDES

Given a plaintext message, the first key is employed to encrypt the plaintext; The second key is also employed to decrypt the encrypted message. Since the second key is not the right key but in a new form, this decryption just scrambles the data further. The twice-scrambled message is then encrypted again with the first key to yield the final ciphertext (10).

According to Alanazi et al, (11), There has always been a suspicion of Triple DES because of how it works, since the origional Algorithm (DES) was not designed to work this way; but no serious flaws have been uncovered in its design.

Weerasinghe et al., (12) proposed a protocol that provides security and privacy services such as user anonymity, message confidentiality, message privacy, user authorization, user authentication, and message replay attacks. The patient is validated with the proposed protocol at the healthcare service to make sure they are registered patient. The identity and medical records of the patient is made anonymous and linked in a single report. The real identity of the patient can be securely reverse tracked: Thus using the temporal identity of the patient to determine his or her real identity.

Chao, Twu, & Shu, (13) proposed a patient-identity security system, that comes with an identity cipher and decipher, and a user-authentication protocol, that will ensure the authentication and confidentiality of patients' electronic medical records (EMRs) at rest and during transit. To sustain the EMR confidentiality, three logical-based functions and a data-hiding function is used by the identity cipher/decipher to encrypt/decrypt a patient's identifying data and medical details in an EMR. The scrambled text of the patient's identifying data is patient-EMR related, whereas that of medical details is healthcare agent-EMR related. The user-authentication protocol which is based on a public key infrastructure (PKI) uses certificates and dynamic cookies for identification/verification in order to support the authentication of an EMR.

Anderson, (14) focused on the move by UK government to centralise patient records whilst putting the security of medical records at risk and will in turn jeopardise patient confidentiality. There are claims that privacy issues will be curtailed by mechanisms in place in the centralized system by way of role based access controls which are expected to limit patient record access by clinicians who claim to have a relationship with patients. This will be done by a page popping up asking the clinician whether they have the consent of the patient to view their medical records. It is very tempting for the clinical staff to click yes in order to view the medical records.

He further explained that they will make use of ‘Sealed Envelops’. This is a feature that will allow sensitive date of patients to be sealed; this is to prevent ordinary clinicians from having access to that sensitive data. If a clinician outsides the care group access the data, an alert is sent to the privacy officer of the care group. There is a further option of the record to be ‘sealed and locked so that clinicians outside the care group will not even know of its existence. They hope to build patient’s confidence by deploying this feature. However, other systems that communicate with the centralised system will have access to the sealed and lock data. Medical records will also be made available upon demand by the law. The data will be 'anonymised' just by merely replacing the name and address with the postcode, date of birth and NHS number. This is a clear indication that the level of confidentiality here is minimal.

(14) proposed the facilitation of the secondary record access where sealing will be accomplished by marking data with HL7 codes which is created for that purpose rather than encrypting the data and keeping the private key on the same patient card.

A critical look at (14) proposal indicates that it is a laudable idea. This is because HL7 facilitates seamless communication between two hospital management systems at the same time making patient records difficult to understand. On the other hand there is a disadvantage with just using the HL7 for data transfer. What happens when a user who is very familiar with the HL7 codes chances upon these sensitive data of a patient? They can easily make meaning out of the HL7 codes. In this case using only HL7 for systems communication is not enough. There should be a way to further make the sensitive data difficult to understand even when you are able to access it.

Benyoucef et al., (2011) investigate the suitability of web service orchestration and choreography, two closely related but fundamentally different methodologies for modelling web service-based healthcare processes. The study showed that Hospital Management systems will have to interact with each other in order to exchange data. Data which is the lifeblood of healthcare is very paramount in the healthcare industry implying that it will have to be available for the right task at the right time. This can be achieved by use of protocols or communication channels such as HL7 (15).

Security was one of the important factors they indicated must be considered for healthcare systems development. This is because models are the blue print of systems; they should represent security features as well.

They also talked about privacy which is currently an issue and requires a lot of attention. They therefore proposed embedding privacy features in modelling languages. Privacy is vital in healthcare as most processes involving interactions with other organizations such as insurance companies, police departments, external laboratories, and other healthcare enterprises, carry private patients’ data as well as private implementation details about internal processes.

The recommendations given above are essential, however, the limitation to the recommendations is the fact that they failed to add a precise solution on how to achieve security and privacy in patient data access and exchange. This is a growing concern to every individual who patronises health services in a way or the other.

One will agree that, the compliance of compulsory standards set by government is not enough to ensure patient confidentiality or data security. More will have to be done to ensure these features in the health care sector (16).

Themistocleous (17), identified that data security and patients' confidentiality are clearly significant challenges to healthcare, and beyond the boundaries organizational structures and roles, specific testing, standards, policies and best practices are needed.

Although the challenges have been identified, there are no solutions to address these challenges. It is apparent that, a lot of researchers are concentrating on how to secure data and by so doing ensure patient confidentiality. It is an established fact that, there is nothing like hundred percent (100%) security. It is difficult to hide data that is accessed every now and then. How do you hide data that is being transferred on a network, or messages that are exchanged by systems? Messages travelling on a network can easily be intercepted by any user on the network. When the data is being transferred using HL7, it becomes quite obfuscated but not completely secure. This is because anybody with the requisite skills in the HL7 codes can make meaning of the intercepted HL7 message. Hence HL7 alone is not the solution to ensuring patient privacy and data security.

To ensure that data intercepted on the network is not used by the wrong person, ETDES Algorithm will have to be implemented. The system sending the HL7 encoded messages will have to encrypt the message at the sending stage. In this case, if any unauthorised user intercepts this message, they cannot make meaning out of the message. They will require a private key to be able to decrypt the encrypted message which is already encoded using HL7 standard. When the message gets to its destination, it will then be decrypted using the private key of the encryption algorithm.

A strong encryption Algorithm will require that it is fully open to public scrutiny and comment to ensure a comprehensive, transparent analysis of the design (18).

Theories backing Encryption

A message in transit or Storage may be protected by encryption (Fig. 2-2). M being the input represents plaintext. The cipher text C= f(K, M), an incomprehensible form of the original plaintext, is computed as a function and a finite secret cipher key K. By applying an inverse transformation M= f^{-1}(K, C), the plaintext may be recovered by the valid receiver from the cipher text. The sender and receiver will both share a secret key K that should be made available only to the two parties using a secured means (19).

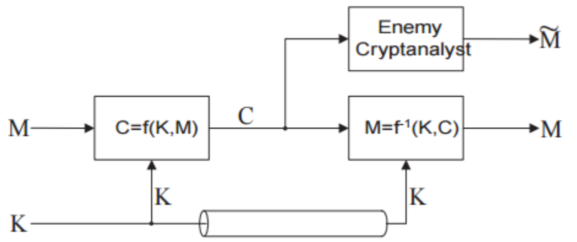


Figure 2-2, source : (19)

Some ciphers are implemented in software, others in Smart-Cards, FPGAs etc. and requires different implementation techniques. A mismatch between the application area, selected cipher, and target technology may decrease the technical efficiency obtained. It is obvious that no matter how efficient and flexible a cipher may be, it will not be optimal enough to meet these challenges. Therefore, a cryptographer will have to implement a cipher that includes general computational process with all construction parameters kept secret; this will make it difficult for a cryptanalyst to solve (19)

The most basic method of attack for any cipher is brute force; where each key is tried until the right one is found. The key length is the determinant of possible number of keys which makes this kind of attack feasible. The strength of an encryption is tied directly to the size of key. Unfortunately, the more the size the more resources required for computation.

Chapple, (20) argued that, encryption is a data-centric security control; it does not protect your physical device but rather prevents unauthorized users from gaining access to your information. Encryption cannot prevent someone from hacking into your system with an inappropriately configured firewall. It will, however, prevent the hacker who gains access to a device from stealing sensitive data.

3. Methodology

This study adopted the design science research methodology in developing a system to meet its objectives. The study explored detailed steps and processes used in the subsequent sections.

ETDES Algorithm

```
Step 1: Start
Step2: Set Private Key=XXXXXXXXXXXX
        Set Hashing = True
Step 3: Get Plain Text
Sep4: Convert Plain Text to Bytes
Step5:  If Hashing=True
                Convert Private Key to Bytes
                Hash Private Key with MD5CryptoServiceProvider
        Else
                Convert Private Key to Bytes
Step6: Set Triple Data Encryption Algorithm (TDES) Key= Hashed Private Key
        Set TDES Mode to ECB
        Set TDES Padding to PKCS7

Step7: TDES.Encrypt(Plain text using Hashed Private Key )
Step8: Release resources used by TDES
Step9: Convert Encrypted Text to Base64
Step 10: Stop
```

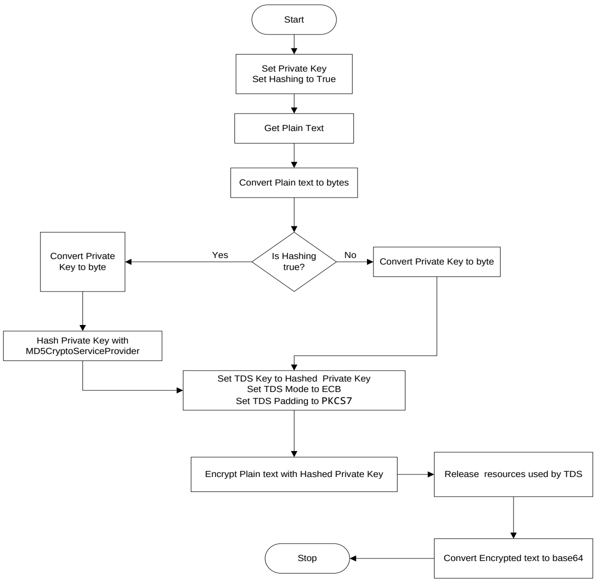

Start
Set Private Key
Set Hashing to True
Get Plain Text
Convert Plain text to bytes
Is Hashing true?
Yes
No
Convert Private Key to byte
Hash Private Key with MD5CryptoServiceProvider
Convert Private Key to byte
Set TDS Key to Hashed Private Key
Set TDS Mode to ECB
Set TDS Padding to PKCS7
Encrypt Plain text with Hashed Private Key
Release resources used by TDS
Convert Encrypted text to base64
Stop

Fig 3-1 Flowchart for the encryption algorithm

ETDES Decryption Algorithm

```
Step 1: Start
Step2: Set Private Key=XXXXXXXXXXXX
        Set Hashing = True
Step 3: Get Cipher Text
Sep4: Convert Cipher Text from Base64
Step5:  If Hashing=True
                Convert Private Key to Bytes
                Hash Private Key with MD5CryptoServiceProvider
        Else
                Convert Private Key to Bytes
Step6: Set TDES Mode to ECB
        Set TDES Padding to PKCS7
Step7: TDES.Decrypt(Cipher text using Encrypted Private Key)
Step8: Release resources used by TDES
Step9: Get Plain Text
Step 10: Stop
```

ETDES Decryption Flow Chart

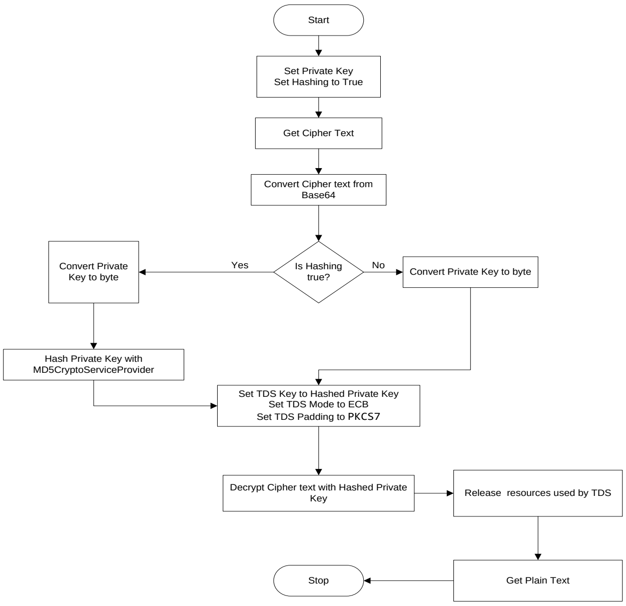

Start
Set Private Key
Set Hashing to True
Get Cipher Text
Convert Cipher text from Base64
Is Hashing true?
Yes
No
Convert Private Key to byte
Convert Private Key to byte
Hash Private Key with MD5CryptoServiceProvider
Set TDS Key to Hashed Private Key
Set TDS Mode to ECB
Set TDS Padding to PKCS7
Decrypt Cipher text with Hashed Private Key
Release resources used by TDS
Get Plain Text
Stop

Fig 3-2 Flowchart for the decryption algorithm

4. Outline of the System

A context level diagram shows the relationship that exists between the system and the external entities that interact directly with the system. It always has the system in the middle with the entities surrounding it (21).

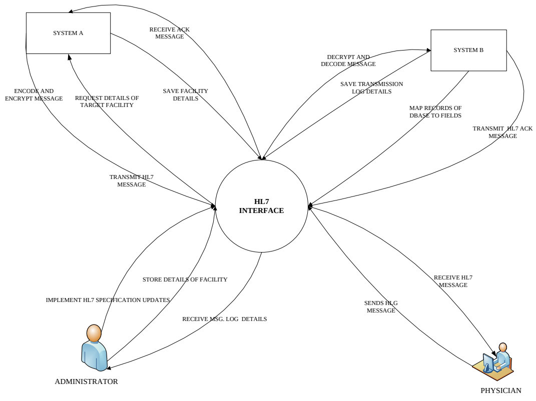

SYSTEM A
RECEIVE ACK MESSAGE
SYSTEM B
DECRYPT AND DECODE MESSAGE
SAVE TRANSMISSION LOG DETAILS
ENCODE AND ENCRYPT MESSAGE
REQUEST DETAILS OF TARGET FACILITY
SAVE FACILITY DETAILS
MAP RECORDS OF DBASE TO FIELDS
TRANSMIT HL7 ACK MESSAGE
TRANSMIT HL7 MESSAGE
HL7 INTERFACE
STORE DETAILS OF FACILITY
IMPLEMENT HL7 SPECIFICATION UPDATES
RECEIVE MSG. LOG DETAILS
RECEIVE HL7 MESSAGE
SENDS HLG MESSAGE
ADMINISTRATOR
PHYSICIAN

Fig 4-1 Context Level Diagram

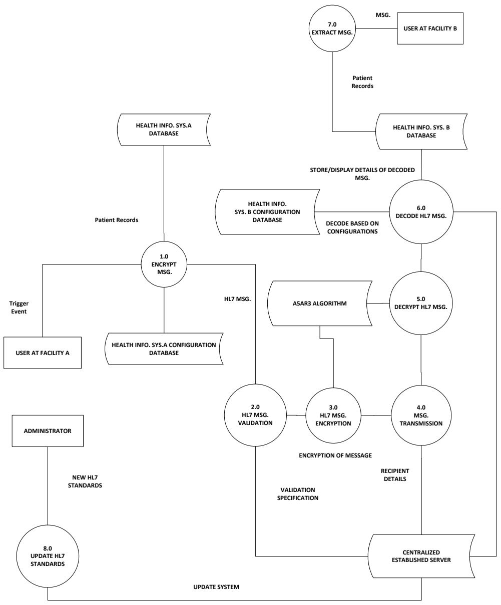
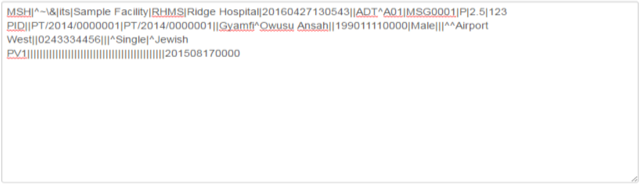


Fig 4-2 data flow diagram of the proposed system

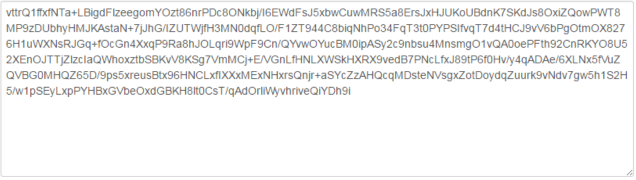
Results



```
MSH|^~\&|its|Sample Facility|RHMS|Ridge Hospital|20160427130543||ADT^A01|MSG0001|P|2.5|123
PID||PT/2014/0000001|PT/2014/0000001||Gyamfi^Owusu Ansah||199011110000|Male|||^^Airport
West||0243334456|||^Single|^Jewish
PV1||||||||||||||||||||||||||||||||||||||||||||201508170000
```

Figure 4-3: Patient's data encoded with HL7 messaging standard

The Figure 4-3 shows patient's data encoded with HL7 messaging standard. It is easy to make meaning out of the encoded message. When this kind of message is transmitted over a network, it can easily be intercepted and interpreted.



vttrQ1ffxfNTa+LBigdFIzeegomYOzt86nrPDc8ONkbj/I6EWdFsJ5xbwCuwMRS5a8ErsJxHJUKoUBdnK7SKdJs8OxiZQowPWT8
MP9zDUbhyHMJKAstaN+7jJhG/IZUTWjfH3MN0dqfLO/F1ZT944C8biqNhPo34FqT3t0PYPSIfvqT7d4tHCJ9vV6bPgOtmOX827
6H1uWXNsRJGq+fOcGn4XxqP9Ra8hJOLqri9WpF9Cn/QYvwOYucBM0ipASy2c9nbsu4MnsmgO1vQA0oePFth92CnRKYO8U5
2XEnOJTTjZIzcIaQWhoxztbSBKvV8KSg7VmMCj+E/VGnLfHNLXWSkHXRX9vedB7PNcLfxJ89tP6f0Hv/y4qADAe/6XLNx5fVuZ
QVBG0MHQZ65D/9ps5xreusBtx96HNCLxfIXXxMExNHxrsQnjr+aSYcZzAHQcqMDsteNVsgxZotDoydqZuurk9vNdv7gw5h1S2H
5/w1pSEyLxpPYHBxGVbeOxdGBKH8It0CsT/qAdOrliWyvhriveQiYDh9i

Figure 4-4: Encrypted Patient's data

Figure 4-4 shows the results of the encrypted patient's data. It is not possible to make meaning out of this cipher text. This will make the patient data secured whilst on transit. A facility can decide to use or not to use SSL/TLS since the data is already encrypted.

The solution proposed by this study makes security a default feature of the HL7 messaging standard.

5. Conclusion

The study employed the use of TDES Algorithm. The private key of TDES Algorithm is crucial for encrypting or decrypting a message, hence the need to protect the key.

The Algorithm was enhanced by first hashing the private key with MD5CryptoServiceProvider (Hence ETDES). The hashed private key cannot be reverse engineered thereby protecting the private key. It is after the hashing of the private key, that it will be used to encrypt the HL7 message.

The decryption process is similar to the encryption process. During the decryption, the private key will have to be hashed before it can be used to decrypted the encrypted HL7 message.

6. Further Work

HL7 is gradually gaining grounds in medical institutions. The focus is always on data at rest; medical facilities concentrate on securing data at rest, whilst securing data on transit is an option. Securing data on transit should be a default feature of the HL7. The study recommends the implementation of ETDES Algorithm with the HL7, which will encrypt the encoded HL7 message before transmission, then decrypt the encrypted HL7 message when it gets to its destination. This will ensure security of data on transit. Medical facilities will not have to worry about employing SSL/TLS. This is because intercepted message will not make meaning to an attacker, thereby protecting patient confidentiality.

References

[1] **Magaqa, Vuminkosi Lionel Longsdale.** researchspace. *researchspace.* [Online] 3 October 2012. [Cited: 15 March 2016.] http://researchspace.ukzn.ac.za/xmlui/bitstream/handle/10413/10383/Magaqa_Vuminkosi_Lionel_Longsdale_2010.pdf?sequence=1.

[2] *A framework for adapting health-level7 techniques in Ghanaian institutions.* **Damoah, D, et al.** s.l. : IEEE, 2014.

[3] *Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia.* **Mweebo, Keith.** Joondalup : Australian eHealth Informatics and Security Conference, 2014. AUSTRALIAN EHEALTH INFORMATICS AND SECURITY CONFERENCE. pp. 35-38.

[4] *The potentials and challenges of big data in public health.* **Vithiatharan, Rena N.** s.l. : Australian eHealth Informatics and Security, 2014.

[5] **HL7.** HL7 International. *HL7.* [Online] February 2011. [Cited: 15 March 2016.] https://www.hl7.org/documentcenter/public_temp_026EC67C-1C23-BA17-0C29030975C47A9B/calendarofevents/himss/2011/HL7%20Organizational%20Backgrounder%20and%20Standards%20Descriptions.pdf.

[6] **Orion, Health.** HL7 Interface Engine. *HL7.com.* [Online] 24 March 2013. [Cited: 15 March 2016.] http://www.hl7.com/interface-engine.html.

[7] **Zero, Division By.** HL7 and security. *dib0.* [Online] 18 January 2011. [Cited: 16 March 2016.] http://www.dib0.nl/code/256-hl7-and-security.

[8] **wikipedia.** Triple DES. *wikipedia.* [Online] 29 March 2016. [Cited: 16 April 2016.] https://en.wikipedia.org/wiki/Triple_DES.

[9] **Tutorialspoint.** Triple DES. *tutorialspoint.* [Online] 28 July 2015. [Cited: 17 April 2016.] http://www.tutorialspoint.com/cryptography/triple_des.htm.

[10] *The DES Algorithm Illustrated.* **Grabbe, Orlin.** 2011, Laissez Faire City Times, pp. 3-5.

[11] *New Comparative Study Between DES, 3DES and AES.* **Hamdan, O, et al.** 2010, JOURNAL OF COMPUTING.

[12] *Patient privacy protection using anonymous access control techniques.* **Weerasinghe, D, et al.** 2008, PubMed, pp. 235-240.

[13] *A patient-identity security mechanism for electronic medical records during transit and at rest.* **Chao, HM, Twu, SH and Hsu, CM.** 2005, PubMed, pp. 1-4,13.

[14] *Under threat: patient confidentiality and NHS computing .* **Anderson, Ross.** 4, s.l. : Emerald Insight, 2006, Vol. 6.

[15] *Modeling healthcare processes as service orchestrations and choreographies.* **Morad, Benyoucef, et al.** 4, s.l. : Business Process Management Journal , 2011, Emerald Insight, Vol. 17, pp. 568-593.

[16] *SOA implementation critical success factors in healthcare.* **Konstantinos, Koumaditis, et al.** 4, Piraeus,Coimbra : Journal of Enterprise Information Management, 2013, Emerald Insight, Vol. 26, pp. 343-349.

[17] *Organizational structures during SOA implementation: the case of a Greek healthcare organization.* **Themistocleous, Konstantinos Koumaditis Marinos.** 3, Aarhus,Piraeus : Transforming Government: People, Process and Policy, 2015, Emerald Insight, Vol. 9, pp. 263-285.

[18]**Rouse, Margaret.** Encryption. *Techtarget.* [Online] November 2014. [Cited: 21 March 2016.] http://searchsecurity.techtarget.com/definition/encryption.

[19]**Dömstedt, Bo and Jansson, Jesper.** The Theory of Dynamic Encryption,a New Approach to Cryptography. *Protego.* [Online] 2001. [Cited: 21 March 2016.] http://www.protego.se/pdf/dyn_enc1.pdf.

[20]**Chapple, Mike.** Data encryption methods: Securing emerging endpoints. *Techtarget.* [Online] April 2010. [Cited: 21 March 2016.] http://searchsecurity.techtarget.com/tip/Data-encryption-methods-Securing-emerging-endpoints.

[21]**Wiegers, Karl.** Requirements Best Practices. *Jamasoftware.* [Online] 26 February 2014. [Cited: 11 April 2016.] http://www.jamasoftware.com/blog/defining-project-scope-context-use-case-diagrams/.

[22]22. *Collaborative development of trusted mashups.* **Ronan, Fox, James, Cooley and Manfred, Hauswirth.** 3, Galway : International Journal of Pervasive Computing and Communications, 2011, Emirald Insights, Vol. 7, pp. 264-284.

[23]*SOA implementation critical success factors in healthcare.* **Konstantinos Koumaditis, Marinos Themistocleous, Paulo Rupino, Da Cunha.** 4, Piraeus,Coimbra : Journal of Enterprise

Information Management, 2013, Emerald Insight, Vol. 26, pp. 343-349.

[24]*Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambi.* **Mweebo, Keith.** s.l. : Australian eHealth Informatics and Security, 2014.

[25]**Peterson, Andrea.** The Switch. *The Washintion Post.* [Online] 20 March 2015. [Cited: 27 August 2015.] https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.

[26]**Press, Associated.** Healthcare Information Technology . *Modern Healthcare.* [Online] 3 August 2015. [Cited: 27 August 2015.] http://www.modernhealthcare.com/article/20150803/NEWS/308029998/indiana-medical-software-company-hack-affected-3-9m-people.

[27]**Howe, Jared.** Resources. *Private Wifi.* [Online] 14 Arpril 2011. [Cited: 27 August 2015.] http://blog.privatewifi.com/a-hacker%E2%80%99s-toolkit/.

[28]**Kioskea.** Data Transmission. *CCM.* [Online] June 2014. [Cited: 18 March 2016.] http://ccm.net/contents/701-data-transmission-transmission-modes.

[29]*An integrated system theory of information security management.* **Hong, Kwo-Shing.** 1, Taiwan : emeraldinsight, 2003, Vol. 7.

[30]**Reina, Veronica.** THE IMPORTANCE OF MEDICAL RECORDS: A CRITICAL PROFESSIONAL RESPONSIBILITY. *Gapmedics.* [Online] 25 March 2014. [Cited: 21 March 2016.] http://www.gapmedics.com/blog/2014/03/25/the-importance-of-medical-records-a-critical-professional-responsibility/.

[31]**Care, Safer Better.** Overview of Healthcare Interoperability Standards. [Online] July 2013. [Cited: 21 March 2016.] https://www.hiqa.ie/system/files/Healthcare-Interoperability-Standards.pdf.

[32]**Microsoft.** HL7 Message Structure. *Microsoft.* [Online] 2015. [Cited: 28 August 2015.] https://msdn.microsoft.com/en-us/library/ee409289.aspx.

[33]**Gilbert, Brian.** What Is A VPN. *What is my IP.* [Online] 2015. [Cited: 23 March 2016.] https://www.whatismyip.com/what-is-a-vpn/.

[34]34. **Wikipedia.** IPsec. *Wikipedia.* [Online] 18 February 2016. [Cited: 23 March 2016.] https://en.wikipedia.org/wiki/IPsec.

[35]35. **Blog, Tech.** The Pros and Cons of Using a Virtual Private Network. *Thrivenetworks.* [Online] July 2015. [Cited: 23 March 2016.] http://www.thrivenetworks.com/blog/2011/07/28/the-pros-and-cons-of-using-a-virtual-private-network/.

[36] *A design Science Research Methodology for Information Systems Research.* **Peffers, Ken, et al.** 2007, Management Information Systems, Vol. 24, pp. 45-78.

[37]**Bord, Jessica De.** Confidentiality. *washington.edu.* [Online] 2013. [Cited: 11 April 2016.] https://depts.washington.edu/bioethx/topics/confiden.html.

[38]**Wikipedia.** Network performance. *Wikipedia.* [Online] 29 February 2016. [Cited: 11 April 2016.] https://en.wikipedia.org/wiki/Network_performance.

[39]**Radatz, Jane, et al.** *IEEE Standard Glossary of Software Engineering.* New York : The Institute of Electrical and Electronics Enginnering, 1990.

[40]**Conn, Joseph.** Healthcare Information Technology. *Modern Healthcare.* [Online] 26 August 2015. [Cited: 27 August 2015.] http://www.modernhealthcare.com/article/20150826/NEWS/150829921/80-of-health-it-leaders-say-their-systems-have-been-compromised.

[41]**Townsend, Patrick.** townsend security. *townsend security.* [Online] 2 April 2013. [Cited: 20 March 2016.] http://info.townsendsecurity.com/why-unprotected-data-business-problem-video.

[42] **Author, Guest.** 5 Consequences of an Information Security Breach. *BestTechie.* [Online] 2 November 2011. [Cited: 20 March 2016.] https://www.besttechie.com/5-consequences-information-security-breach/.

[43]**Beal, Vangie.** encryption. *Webopedia.* [Online] 5 April 2001. [Cited: 20 March 2016.] http://www.webopedia.com/TERM/E/encryption.html.

[44]**HL7, About.** About HL7. *HL7.* [Online] 17 June 2010. [Cited: 21 March 2016.] http://www.hl7.org/about/index.cfm?ref=common.

[45]**Sookasa, Resources.** Resources. *Sookasa.* [Online] 11 April 2015. [Cited: 23 March 2016.] https://www.sookasa.com/resources/HIPAA-encryption/.

[46]**Techopedia, TDES.** Triple DES. *techopedia.* [Online] 13 Januar 2012. [Cited: 09 April 2016.] https://www.techopedia.com/definition/4144/triple-des.

[47]**techopedia.** Data Transfer. *techopedia.* [Online] 2 April 2013. [Cited: 16 March 2016.] https://www.techopedia.com/definition/18715/data-transfer.

[48] **Wieringa, Roel.** ntroduction to design science. *refsq.org.* [Online] 4 August 2013. [Cited: 11 April 2016.] https://refsq.org/wp-content/uploads/2013/05/Wieringa-2013-REFSQ-DS-Introduction-to-design-science-methodology-slides.pdf.

[49]49. **Cod, Confidentiality.** Confidentiality, Patient/Physician. *Aafp.* [Online] 2013. [Cited: 11 April 2016.] http://www.aafp.org/about/policies/all/patient-confidentiality.html.

[50]**Manes, Casper.** Security 101: at rest or in transit – protecting data with encryption. *gfi.com.* [Online] 19 December 2014. [Cited: 11 April 2016.] http://www.gfi.com/blog/protecting-data-with-encryption/.

[51]**Shackleford, Dave.** Regulations and Standards:Where Encryption Applies. *sophos.* [Online] May 2014. [Cited: 11 April 2016.] https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/PublicSectorBenelux/sophos-encryption-regulations-standards-wpna.pdf?la=en.

[52]**Shephard, David.** 84 Fascinating & Scary IT Security Statistics. *NetIQ Communities.* [Online] 16 March 2015. [Cited: 21 April 2016.] https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/.

[53]**Stallings, William.** NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS FOURTH EDITION. *Prentice Hall.* [Online] 2011. [Cited: 11 April 2016.] http://sbmu.ac.ir/uploads/3._Network-security-essentials-4th-edition-william-stallings.pdf.

[54]**Rouse, Margaret.** Pivate Key. *Techtarget.com.* [Online] 2007. [Cited: 09 April 2016.]

http://searchsecurity.techtarget.com/definition/private-key.

[55] Hashing. *Techtarget.* [Online] September 2005. [Cited: 09 April 2016.] http://searchsqlserver.techtarget.com/definition/hashing.

[56]**Sparx, Systems.** The Use Case Model. *Sparx Systems.* [Online] 2004. [Cited: 28 04 2011.] http://www.sparxsystems.com.au/resources/tutorial/use_case_model.html.

[57]**Abdul-Malik, Shakir.** HL7. *Slideshare.* [Online] January 2011. [Cited: 5 May 2016.] http://www.slideshare.net/AShakir/hl7-v2-messaging-conformance-jan-2011.

[58]**Staggers, Nancy, Weir, Charlene and Phansalkar, Shobha.** NCBI. *NCBI.* [Online] 2008. [Cited: 15 March 2016.] http://www.ncbi.nlm.nih.gov/books/NBK2644/#_ch47_rl1_.

[59]**Thakur, Dinesh.** Data Transmission. *Computer Notes.* [Online] 22 June 2013. [Cited: March 2016.] http://ecomputernotes.com/computernetworkingnotes/communication-networks/data-transmission.

[60]*Data Integrity and Security: Who's in Charge Here Anyway?* **Weiss, Kenneth P.** 4, s.l. : Emerald Insight, 1993, Vol. 1.

[61] *A DESIGN THEORY FOR INFORMATION SECURITY AWARENESS.* **Petri, Puhakainen.** s.l. : A Scientiae Rerum Naturalium 463, 2006.

[62]*Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia.* **Mweebo, Keith.** Joondalup : Australian eHealth Informatics and Security Conference, 2014. AUSTRALIAN EHEALTH INFORMATICS AND SECURITY CONFERENCE. pp. 35-38.

[63]**Mahan, RE, et al.** Secure Data Transfer Guidance forIndustrial Control and SCADA Systems. *PNNL.* [Online] September 2011. [Cited: 18 Marh 2016.] http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

[64] *Security Threats to Internet: A Korean.* **Jung, B, Han, I and Lee, S.** s.l. : Information & Management, 2001, Vol. 38.

[65]**Hayaati, Najwa and Mohd, Alwi.** E-LEARNING STAKEHOLDERS INFORMATION SECURITY VULNERABILTY MODEL. *cranfield.* [Online] 2012. [Cited: 20 March 2016.] https://dspace.lib.cranfield.ac.uk/bitstream/1826/7387/1/Najwa_Hayaati_Mohd_Alwi_Thesis_2012.pdf.

[66]**Bray, Thomas J.** Encyclopedia of Information Assurance. *tandfonline.* [Online] 7 January 2011. [Cited: 20 March 2016.] http://www.tandfonline.com/doi/abs/10.1081/E-EIA-120046566#.Vu683uKLTbg.

[67] *Online Security Performances and InformationSecurity Disclosures.* **Li, David C.** 2, s.l. : Journal of Computer Information Systems, 2015, Vol. 55.

[68]*Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA.* **Burkett, Jason S.** 1, s.l. : Information Security Journal: A Global Perspective, 2012, Vol. 21.

[69]*Information Security Awareness Status of Business College: Undergraduate Students.* **Kim, Eyong B.** 4, s.l. : Information Security Journal: A Global Perspective, 2013, Vol. 22.

[70]**Behrens, Matt.** Understanding the 3 Main Types of Encryption. *Atomic Object.* [Online] 20 November 2014. [Cited: 20 March 2016.] https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/.

[71]**Marinič, Milena.** The Importance of Health Records. *Scientific Research Publishing.* 20 May 2015, p. 617.

[72]**Com, SSL.** What is SSL. *SSL.* [Online] 26 October 2015. [Cited: 23 March 2016.] http://info.ssl.com/article.aspx?id=10241.

[73]**HL7.** Encryption. *HL7.* [Online] August 2007. [Cited: 23 March 2016.] http://wiki.hl7.org/index.php?title=Implementation_FAQ:Encryption_and_Security.