Next Generation Cyber Security Solution for an eHealth Organization

Hossam Ahmed[1], Abeer Alsadoon[1], P.W.C. Prasad[1], N. Costadopoulos[1], Lau Siong Hoe[2], Amr Elchoemi[3]
[1]Charles Sturt University Study Centre, Sydney, Australia
[2]Multimedia University, Malaysia
[3]Walden University, USA

***Abstract*—eHealth organizations are a major target for hackers as they hold wealth of information. Current cyber security solutions for eHealth organizations are not comprehensive and only protect certain security layer. Therefore; the need for a next generation cyber security solution is increasing, a solution that is smart, scalable and adoptable to challenges. The wide spread of security tools and advancing technology have provided the needed infrastructure to create a comprehensive eHealth security solution. Connecting the right security tools together to ensure the overall security without affecting the network performance and user productivity is hard and requires special setup. The network layer is a major target for any eHealth organization, this research has indicated several network security metrics that need to be considered when designing and managing network security for an eHealth organization. The ultimate goal of this research is to identify the limitations in the current eHealth organization cyber security solutions specially the network layer and propose a next generation cyber security solution for eHealth organizations.**

Keywords— eHealth, Cyber Security, Next Generation, Defense in Depth

I. INTRODUCTION

Cyber-attacks are increasing rapidly as hackers have evolved to be smarter, and technology more complex. The financial and reputational consequences from a cyber-attack or breach can be devastating to any organization specially eHealth organizations [1] [2]. Today's eHealth systems need to deal with a new and different level of patient doctor interactions and they pose new kinds of challenges and threats to security and privacy. With increasing number of eHealth systems that are being built on mobile, web and cloud platforms, providing effective security and privacy has become a major concern [3]. It is crucial not only to reduce costs, improve healthcare and patient safety. However, to achieve that they require health organizations to share and exchange clinical sensitive information within a robust privacy-preserving environment [4] [5]. To protect the eHealth organization, the solution should be able to monitor and control all security aspects of an eHealth organization [6] [7]. A new implementation of digital patient records, electronic management records, risk management, security tools, big data and all elements needed for better data security. Health care organizations are quickly confronting security dangers and vulnerabilities through the implementation of digitalization of patient records [8] [9]. Security is defined as the extent to which this personally identifiable information (PII) can be stored and shared in such a manner that access to the information is limited to authorized parties and protected through the security layers [10] [11].

II. LITERATURE REVIEW

A. Cyber Security in e-Health

Health care organizations are quickly confronting security dangers and vulnerabilities through the implementation of digitalization of patient records [12]. The definition of privacy emphasizes the control over the personally identifiable information (PII) that should always rest with the data. Taking control over this information from the subjects removes the user privacy.

Current analysed solutions pose various limitations, such as slow time for data access [13], complex configuration and the need for extra resources to manage and analyse the data and network [14], ignoring the infrastructure proper setup to support the eHealth organization IT system or incorporating too many applications that adds overheads on the network and management [15].

Defense in Depth (DiD) is a multi-layer security controls and mechanisms that are placed throughout the eHealth organization IT system [16]. DiD usually uses access control and mechanisms to identify user interaction, methods of access, host security, application security, network level security, data security and security auditing. DiD is utilised in the proposed enhanced solution to protect the eHealth network layer through creating multi-tier network, use strong encryption (SSL) for data transfer, use centralised login and next generation firewalls, IDSs and malware analysis.

B. Current Best Solution

The architecture proposes an agent-oriented architecture that uses one-directional hashing (MD5) for the sharing of sensitive data, where agents integrate with information systems (e.g. Medicare) and handles data transfers and the levels of encryption of data where only destination organizations can re-identify. Each agent has the full authority to determine its action with respect to data. When data originates from another organization, the source-organization sends data in a data-bucket (DB), which includes four elements:

ISBN: 978-1-5090-4911-0 (c) 2017 IEEE

DB=<PE, DE, OIK, LoE>

PE= Protocol Element DE= Date Element,

OIK= Organization ID Key LoE= Level of Encryption

The architecture poses three limitations; firstly, with large databases, using the sequential execution of the security algorithm (SEC) can cause a bottleneck and slow down the performance. Secondly, using different agents for each eHealth organizations is limiting the scalability of the overall architecture. Lastly, the architecture used MD5 for encryption. MD5 is known as hashing algorithm and can be easily cracked and decrypted. MD5 has known security flaws and vulnerabilities and is based on a very old algorithm. MD5 is considered broken nowadays as it can easily generate collisions. The architecture didn't propose the use of salting with MD5, salting would have made it a bit more resilient.

III. PROPOSED MODEL

A. *Proposed Enhanced Next Generation Cyber Security for e-Health*

The proposed solution is presented in Figure 1 and it covers and rectifies the current limitations in the best selected solution by removing the need for different communication agents, utilizing unified communication method (HTTPS), protecting data transfer using secured communication (HTTPS with SSL) and using strong encryption algorithm (RSA 2048) to secure the data transmission. The use of unified communication agent will allow the organizations to scale easily and quickly without the need for change or adopting a new agent and removing any complex configuration. Secure transmission method (HTTPS with SSL) is used is to keep sensitive eHealth information sent across the Internet encrypted so that only the intended recipient can understand it.

This is important because the information sent on the network or internet is passed from computer to computer to get to the destination. When HTTPS with SSL is used, the information becomes unreadable to everyone except for the destination you are sending the information to. This protects it from hackers and identity thieves. In addition, the use of a proper SSL certificate will also provide authentication. This means eHealth data transferred inside the network or over the internet are more protected and only authorized destinations will be able to receive the data and read it, this ensure the data integrity. Compared to MD5, RSA is considered a very strong encryption algorithm. RSA utilize private and public keys, private keys never need to be transmitted or revealed to anyone, only public keys are shared. Another major advantage of RSA encryption is that they can provide digital signatures that cannot be repudiated. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. Thus, a sender can repudiate a previously authenticated message by claiming the shared secret was somehow compromised by one of the parties sharing the secret.

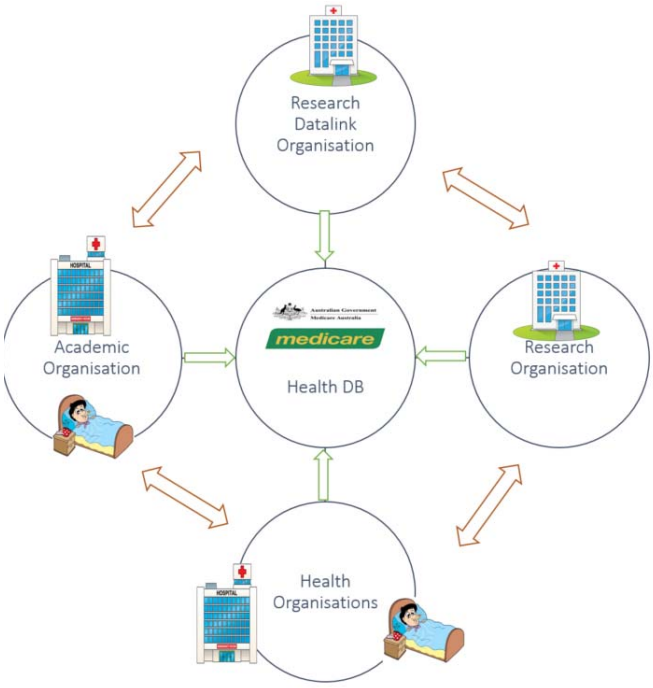

Fig. 1. proposed next generation cyber security solution for an eHealth organization

B. *Proposed Enhanced Next Generation Cyber Security for e-Health*

Here lies the opportunity to design an advanced security platform for eHealth organization that exemplifies a next generation cyber security service (Figure 3 and 4). Using the above mentioned unified secure communication method, along with strong encryption achieves a great security of data communications, however we still need to protect the eHealth network and data at other time. To achieve that, we broke down the network of an eHealth organization into three tiers (private network, internal network, external network) as per (Figure 2 and 3).

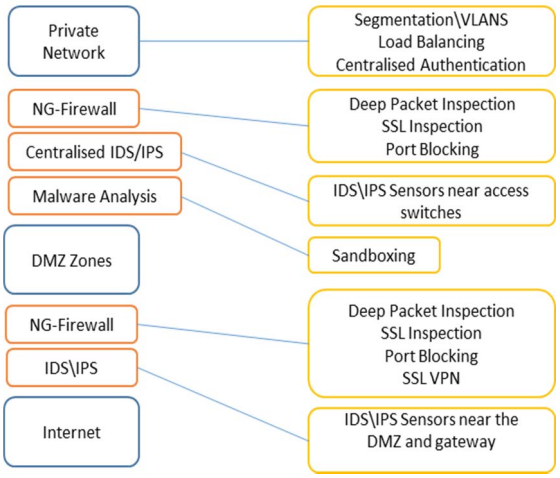

Fig. 2. Proposed enhanced next generation cyber security solution for an eHealth organization

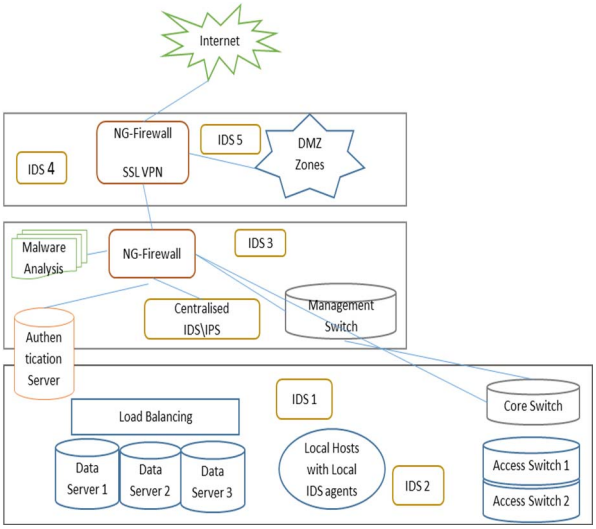

Fig. 3. Proposed enhanced next generation cyber security solution for an eHealth organization (Network Diagram)

The private network will include data server with load balancing, centralised authentication server, cores switch, access switch and hosts computer. Data servers will include load balancer to manage the eHealth data access and provide redundancy to ensure high availability of the eHealth data. For authentication, we will use a centralized server (MS Active Directory) to manage roles and permissions access for all users including doctors, nurses, admin and remote users to the network and eHealth data. The use of a core switch with VLANs to segment the network and increase the security by separation the data, control and management packets. Also, the core switch will act as the medium between the private network and internal network so all traffic can be monitored using an IDS connected on a SPAN port.

Access switches will be used as a stack with failover to provide redundancy on the network to ensure high network availability which is vital for any eHealth organization. We will also use VLANs on access switches to segment the network and manage data and network access and to provide extra security to mitigate any attack or breach by removing only the attacked segment. Internal network will include, next generation firewall with direct link to the authentication server, IDS\IPS server and sensors, malware analysis with sandboxing and management switch.

The next generation firewall will be connected directly to the private network core switch to provide deep packet inspection and ACL, connected directly to the External network NG-Firewall to provide an extra inspection point, connected to the centralised IDS\IPS server to receive direct alerts, connected to the malware analysis to forward suspicions packets and receive results and connected to the authentication server (MS Active Directory) to forward authentication requests.

The centralised IPS\IDS will communicate directly with IDS\IPS sensors to receive alerts and communicate to the firewall to forward alerts and check against ACL rules. Malware Analysis, is the big addition to the solution, currently all suspicion activities are being detected based on signatures or the network behaviour. As the attackers are getting smarter they found a better way to include the malware files within a legitimate packet. Malware analysis will live-inspect those packets and run them on a locked and secure environment and test their activity then report it back to the firewall so it can allow or deny the packet based on the results. Lastly, the management switch will allow centralised management of the core switch and access switches.

The external network of the eHealth organization will include next generation firewall with SSL VPN service, IDS\IPS sensors and DMZ zones. DMZ Zones will include servers that needs to be accessed from the internet that is separate than the internal network. IDS\IPS Sensors will be located near the DMZ zones to monitor the traffic and report it to the IDS\IPS centralised server.

SSL VPN will provide secure remote access for eHealth organization users and will be connected to the authentication server via the internal network NG-Firewall to provide role and permission access control for remote users. Next generation firewall will be connected to the internet link to allow inbound and outbound traffic and provide deep packet inspection and act as the first interface to protect the eHealth organization network from external attacks. It will be configured with DMZ zones, for eHealth organization that allow access to web services. This ensures isolation between external network and internal network. It will also be connected to internal network NG-Firewall to forward inbound traffic and receive outbound traffic, provide packet routing, inspection and SSL encryption\decryption.

C. *Encription Algorithm Evaluation*

In the section, we evaluating the difference between RSA and MD5 (Table 1) to contrast the difference of resiliency against most common attacks. Also, evaluating the speed of encryption and decryption (Table 2) between common RSA key sizes to determine the best key size.

RSA offers many key sizes for data encryption, a comparison (Table 2) between the following keys (512, 1024, 2048, 4098, 8192) has shown that 2048 key size is very resilient and fast compared to other key sizes. 2048 has an average of 2.92 millisecond for encryption and average of 9.097 for decryption [17].

IV. Experemental Results and Evaluation

HTTPS offers a great transfer speed compared to HTTP without the use of caching. Any encrypted data can't be cached and that applies to eHealth data. Every connection would have a unique session and every transfer would have a different sequence and encryption. A comparison (Table 3) between HTTPS and HTTP shows that without any caching and using the same network speed, HTTPS provide faster data transfer speed than HTTP. The overall speed varies between (79% to 48%) for file sizes from 100 KB to 100 MB (Figure 4). That means the eHealth data is not only secure but also the data transfer rate is much faster. This is very helpful for any

eHealth organizations where accessing the data is very critical and any delays could mean loss of life.

Algorithm: Data Transfer
DB = DS + LS
EDS = DS + RSA 2048
DT = HTTPS + ED + LS

TABLE 1 – CRYPTOGRAPHIC ATTACKS TIME FOR THE CURRENT ALGORITHM (CA) AND PROPOSED ALGORITHM(PA)

Algorithem Type	File Size	Ciphertext Only Attacks (COA)	Known Plaintext Attack (KPA)	Chosen Plaintext Attack (CPA)	Dictionary Attack	Brute Force Attack (BFA)	Man in Middle Attack (MIM)	Side Channel Attack (SCA)
CA	100 Kb	.1	.5	1	1	1	.1	.5
PA	100 Kb	10	15	12	60	120	.1	90
CA	1 Mb	.5	.7	1	1	1	.1	.7
PA	1 Mb	50	25	30	60	120	.1	140
CA	5 Mb	.6	.7	1.2	1	1.2	.1	1.5
PA	5Mb	250	100	150	300	600	.1	590
CA	10 Mb	.9	.9	2	2	3	.1	1.8
PA	10 Mb	1250	500	750	1500	300	.1	3000
CA	20 Mb	1.5	1.2	2	2	3	.1	2
PA	20 Mb	6250	2500	3750	7500	1500	.1	15000
CA	50 Mb	2.2	1.9	3	3.5	4.8	.1	3.4
PA	50 Mb	31250	12500	18750	37500	7500	.1	75000
CA	100 Mb	2.6	2.7	3	5.0	8	.1	10
PA	100 Mb	31250	12500	18750	37500	7500	.1	75000

TABLE 2 - ENCRYPTION AND DECRYPTION TIME FOR RSA DIFFERENT KEY SIZES

RSA Key Size	Encryption (Milliseconds)	Decryption (Milliseconds)
512	.51	.426
1024	1.03	1.644
2048	2.92	9.097
4096	10.05	61.549
8192	37.79	151.517

TABLE 3 – HTTP VS HTTPS DATA TRANSFER SPEED IN SECONDS WITH NO CACHING.

File Size	Transfer Speed (Seconds)	Difference HTTP-HTTPS (Seconds) (Percentage)
Current Method (HTTP)		
100 Kb	2.302	+1.817 (21% slower)
Proposed Method (HTTPS)		
100 Kb	.485	-1.817 (79% faster)
Current Method (HTTP)		
1 Mb	20.719	+19.894 (39% slower)
Proposed Method (HTTPS)		
1 Mb	.8245	-19.894 (61% faster)
Current Method (HTTP)		
5 Mb	85.640	+81.518 (48% slower)
Proposed Method (HTTPS)		
5Mb	4.122	-81.518 (52% faster)
Current Method (HTTP)		
10 Mb	171.281	+163.036 (48% slower)
Proposed Method (HTTPS)		
10 Mb	8.245	-163.036 (52% faster)
Current Method (HTTP)		
20 Mb	342.562	+326.072 (48% slower)
Proposed Method (HTTPS)		
20 Mb	16.490	-326.072 (52% faster)
Current Method (HTTP)		
50 Mb	856.406	+815.182 (48% slower)
Proposed Method (HTTPS)		
50 Mb	41.224	-815.182 (52% faster)
Current Method (HTTP)		
100 Mb	1712.812	+1630.362 (48% slower)
HTTPS		
100 Mb	82.450	-1630.362 (52% faster)

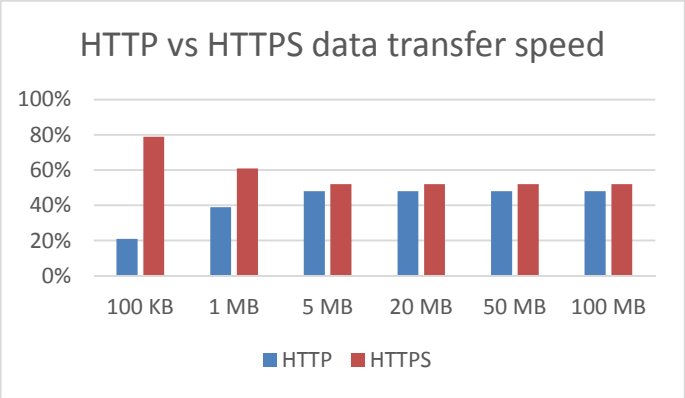

Fig. 4 HTTP vs HTTPS data transfer chart

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain. Hence, the attacker applies maximum effort towards finding out the secret key used in the cryptosystem.

Once the attacker is able to determine the key, the attacked system is considered as broken or compromised. Based on the methodology used, using RSA instead of MD5 for encryption has proven to increase the security [20], a

comparison (Table 2) between RSA and MD5 against common attacks has proven that RSA is very resilient in protecting eHealth information. To decrypt a 100 KB file that is encrypted using RSA, an average of 10 days or more is needed, while 100 KB file that is protected using MD5 can be decrypted in less than a day using a standard computer with the following specs (I7 processor, 8G RAM, SSD Hard Disk). As per the (Table 2), the RSA algorithm is proven solid against common types of attacks expect Man in the Middle Attack (MiM). This attack the hacker doesn't crack the algorithm itself, but intercept the connection.

V. Conclusion and Future Work

Security in eHealth should maximize the health care quality and minimize the eHealth care cost [18]. In this research, we have proposed a next generation cyber security solution using Defense in Depth technique that provides security for eHealth organizations. This research focuses on securing eHealth organization from attacks targeting the network. By implementing multi-tiers network layers and using next generation security tools to identify the current threats and vulnerabilities, block them and protect against zero-day vulnerabilities and smart malwares. Threats need to penetrate not only the external network of the eHealth organization but three networks to reach to the eHealth organizations data. The dynamic multi-tier network elements require attackers to reacquire targets, increasing the cost of an attack and decreasing the amount of time an attacker has to exploit threat. This solution provides feasible effective measurements for an eHealth organization network security while at the same time providing the information of how security products would most enhance that organization's security posture.

Current solution limitations come from the use of a weak encryption algorithms as well as the lake of unknown and zero-day threats. Those limitations are very significant for any eHealth organizations where patient data can be captured or leaked. That's why the use of a strong encryption while the data is in transit is very critical as well as the use of Malware Analysis to identify any suspicious behaviour.

Future work. Malware Analysis is an important part of preventing and detecting future cyber-attacks on eHealth organizations. Using malware analysis tools, cyber security experts can analyse the attack lifecycle and glean important forensic details to enhance eHealth threat intelligence, advancing the malware analysis techniques and tools ensures that eHealth organization can defend against zero-day vulnerabilities and protect the patient and other staff personal identification information [19]. Also, enforcing and advancing the encryption techniques and algorithms ensure the integrity of the data and ensure that PIIs and other data are kept safe while in transit or at rest.

References

[1] M. Farzandipour, F. Sadoughi, M. Ahmdi and I. Karimi, "Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study," p. 34, 2010.

[2] M. Rahimi and M. Hayeri Khiyavi, "Security Serum injection model in application level for next generation network," International Conference on Cyber-Crime Investigation and Cyber Security ICCICS, pp. 22-40, 2014.

[3] P. Mehndiratta, S. Sachde and S. Kulshrestha, "A Model of Privacy and Security for Electronic Health Records," Springer International Publishing, pp. 202-213, 2014.

[4] A. Taweel, S. Mahmoud and A. R. Tawil, "Privacy-Aware Agent-Oriented Architecture for Distributed eHealth Systems," Springer-Verlag Berlin Heidelberg, pp. 418-427, 2014.

[5] A. Rath and J. Colin, "Towards purpose enforcement model for privacy-aware usage control policy in distributed healthcare," Int. J. Security and Networks, pp. 1-12, 2013.

[6] R. Zhang and L. Liu, "Security Models and Requirements for HealthCare Application Clouds," IEEE 3rd International Conference on Cloud Computing, pp. 268-275, 2010.

[7] J.C. Lee, & D.S. McCrickard, "Towards Extreme(ly) Usable Software: Exploring Tensions Between Usability and Agile Software Development," Agile 2007, pp. 59-71, 2007.

[8] L. Barua and Shen, "Secure personal health information sharing with patient-centric access control in cloud computing," 2013 IEEE Global Communications Conference (GLOBECOM), pp. 647-652, 2013.

[9] V. Liu, A. D. Tesfamicael, W. Caelli and T. Sahama, "Network Security Metrics and Performance for Healthcare Systems Management," 17th International Conference on E-health Networking, Application & Services (HealthCom2015), pp. 2-7, 14-17 October 2015.

[10] A. Soceanu, M. Vasylenko, A. Egner and T. Muntean, "Managing the Privacy and Security of eHealth Data," 2015 20th International Conference on Control Systems and Computer Science, pp. 439-446, 2015.

[11] S. Stolfo, S. Bellovin and D. Evans, "Measuring security," 2013 47th International Carnahan Conference on Security Technology (ICCST), pp. 1-5, 2011.

[12] N. M. Shrestha, Abeer Alsadoon, P. W. C. Prasad, L. Hourany, A. Elchouemi, "Enhanced e-Health Framework for Security and Privacy in Healthcare System," 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 75-79, 2016.

[13] Lee, K. C., Integrating scenario-based usability engineering and agile software development, Virginia Polytechnic Institute and State University, 2007.

[14] S. Gorat, J. Tront and R. Marchany, "Advancing the Defense in Depth Model," 2012 7th International Conference on System of Systems Engineering (SoSE), p. 6, 285-290 2012.

[15] M. H. Khyavi and M. Rahimi, "Conceptual model for security in next generation network," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 591-595, 2016.

[16] N. Boggs, S. Du and S. J. Salvatore, "Measuring Drive-by Download Defense in Depth," Springer International Publishing Switzerland, 2014.

[17] A. Alrasheed and F. , "RSA Attacks," University of Tennessee.

[18] M. Huda, S. Yamada and N. Sonehara, "Privacy-aware access to patient-controlled Personal Health Records in emergency situations," 009 3rd International Conference on Pervasive Computing Technologies for Healthcare, pp. 1-6, 2009.

[19] O. Sohaib, & K. Khan, "Integrating Usability Engineering and Agile Software Development: A Literature Review," 2010 International Conference On Computer Design And Appliations, pp. V2-32-V2-38, 2010.