International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Threat Modeling of Electronic Health Systems and Mitigating Countermeasures

John K. Alhassan[1], Emmanuel Abba[1], O. M. Olaniyi[2], and Victor O. Waziri[1]
[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[2]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
jkalhassan@futminna.edu.ng

***Abstract*—Electronic health systems (EHS) serve as information management systems for health records of patients which are various data generated from interactions between patients and medical personnel. The security of electronic health system is vital due to the growing acceptance of their use. There is a need to assure users that the data generated and stored on the EHS are protected from adversaries. In the case where the data is already compromised, it is imperative to locate the source of the threat as quickly as possible and implement appropriate countermeasures against such vulnerabilities starting from the highest vulnerable point to lower vulnerabilities. In this study, a threat security model for the EHS was proposed from identified threats which were then discussed. Based on these threats, possible counter measures for authentication and authorization control were highlighted. The threat model was developed through a procedure that guarantees the integrity, availability and confidentiality of health records. The procedure involves using the STRIDE threat modelling tool to identify potential threats which were then ranked with respect to the amount of risk they pose to the system based on scores calculated using DREAD; a threat-risk rating model. The result is a collection of identified and rated threat in order of decreasing risk to an EHS. Careful consideration of the resulting threat rating model by information system security professional will lead to the development of secure systems and provide a guide to the order in which vulnerabilities should be patched in compromised existing systems.**

Keywords-threat modeling; electronic health system; countermeasures; attacks; authentication; authorization

I. INTRODUCTION

e-Health systems (EHS) were introduced to facilitate health care delivery and health records management as a result of inadequate facilities to cater for the teeming population of people in need of qualitative health care services. e-Health systems have improved workflow for healthcare providers and increase patients access to health care by providing a user friendly and reliable means by which patients can interact with heath care service providers [1]

The application of information technology in the provision and management of health administration is constantly advancing as the quality of patient care in recent times rely upon timely collection and processing of patients clinical information [2]. Sharing of patient healthcare information is happening more rapidly and the process is getting reliable with advancement in technology. These has led e-health care to become critical for achieving better operation of adequate health care services with lower operation costs and efficient service delivery [3].

However, such sharing of healthcare information requires to be done securely in a manner that guarantees privacy as required by law. It is obvious that health management systems process and store very delicate data about a patient's health status and should have an appropriate privacy framework because the revelation of health records may result in stern social effect on patients. Exposing patient's confidential health data outside the e-health system, accidentally or deliberately, must be prevented by healthcare professionals or information technology service providers who will face stern legal punishments for violating privacy laws [4].

The threats faced by EHS may lead to the disclosure of private health data and violation of privacy laws. These threats may be classified as authentication, accounting and authorization threats as generally known to other management information systems such as banking and manufacturing. Securing this areas of E-Health involves information security and privacy as well as physical safety [5].

Continuous monitoring of e-health systems provides a steady stream of data that can be used to identify and correct security deficiencies as the system is developed, tested and used to get ahead of the problem posed to e-health, this can be done to determine threat and attacker behavior in order to anticipate when and how it may happen and preparation of adequate counter measures as may be required to prevent such occurrences. This is done in a process referred to as threat modelling [6]; a systematic process of identifying and rating threats [7]. The key to establishing an effective threat model for any information system is prior determination of where the vulnerabilities exist and more security should be implemented to ensure the system is secure [8]. These vulnerable parts of the system are variables that change as new factors that may pose threats evolve and get detected.

The procedure for threat modeling [9] optimizes network security by recognizing targets and vulnerable points in the system and then implementing a plan for countermeasures to mitigate the results of exploiting these threats to the system.

In the case of an e-health system, a threat is any action or event that may lead to malfunction of the system and services it provides or to patient health record data disclosure or incidental such as the failure of a patient's medical device, and that can compromise the confidentiality, integrity and availability of the system.

While formulating the security requirements for an EHS, the threats are analyzed based on how critical they are and likelihood that they may occur, and a resolution to either mitigate the threat or accept the associated risk is made because definitions of the functionalities and requirements for EHS are constantly evolving as knowledge and experience with these tools increase [4]. Modelling threats and security requirements provide the foundations upon which security controls for the EHS is designed and implemented [10]. Identifying threats helps develop realistic and meaningful security requirements which will be used to come up with the threat model. This is particularly essential because if the security requirements are faulty, the definition of security for that EHS is faulty, the threat model is faulty and thus the EHS cannot be secure. After the threats are Identified, they are rated according to the degree of risk that they pose to the system. The vulnerabilities that are likely to cause a much larger damage are rated as high and those that are low risk are rated as such.

The requirement definition for the development of Secure EHS follows from the premise that system should be convenient, usable and most importantly trustworthy, and secure patient private information. Proper identification and rating of threats on these requirements define the functionality and service the system will provide and thus appropriate selection of countermeasures that reduce the ability of attackers to misuse the system. In that respect, threat modeling looks at the system from the perspective of an adversary to help designers anticipate various attack goals and determine answers to questions about what the system is designed to protect, and from whom. Rating the threats ensures that for already existing systems, when the need arises to patch vulnerabilities in the system, security professionals will know where to start from. This study builds on the identification of threats done using STRIDE threat model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) to identify potential threats which were then rated based on the security risk posed using a DREAD (Damage potential, Reproducibility, Exploitability, affected users, and Discoverability) risk rating model.

The remaining section of the paper is organized into five sections: Section II presents the review of related works; the methodology for modelling e-health system is presented in section III; results are discussed in IV, Section V proposed possible countermeasures to identified threats in while Section VI concludes the paper and open our next direction in future research endeavor.

II. REVIEW OF RELATED WORKS

The application of information technology for providing health care and medical data privacy has a number of related works in literature.

[11] modeled threat evaluation for dynamic targets using Bayesian network approach. A range of various parameters were considered to build the Bayesian model. They proposed that a target to a defended asset is clearly related to both the intent parameters and capability. The authors stated that the range of a target's weapon systems, the gap between the target and the assets being defended are interrelated, since a target is more threatening to a defended asset if the defended asset is within the range of its weapon systems, than if it is outside it. The threat evaluation system they implemented can be applied to an air defense scenario and can enable in radar, aircraft, etc. The authors however focused only on outsider threats and threats posed by weapons and payed no attention to threats that may arise as a result of insider action such as sabotage or spies and espionage.

[12] presented a research on an automated system for managing patient information and its administration with a view to eliminate the problem of inappropriate data archiving, inaccurate reports, time wastage in storing, processing and retrieving information encountered by the traditional hospital system in order to improve the overall efficiency of the organization. The method used to implement the system was system requirement analysis, system design and development using appropriate programming language. However, no threat model was used to plan security implementations for the system and they failed to address threats that may affect the system developed or indicate in any way that it was a concern that needs to be addressed.

In [13] the authors proposed a quantitative methodology to rank the threats in a cloud environment using Microsoft's STRIDE-DREAD model to assess existing threats in cloud environment and measure the consequence of these threats. The threats they identified were ranked based on the nature of its severity and also giving a high priority to clients' requirements on the perspective of security. They stated that their methodology would serve as a tool for guiding security experts and software developers to continue with securing process especially for a private or a hybrid cloud. After ranking the threats, the authors provided a link to a well-known security pattern classification. They however failed to provide any over-weighting for client's requirement, as these requirements would have been an implemented security protocol in the system.

A STRIDE-based Security Architecture for Software-Defined Networking was presented in [14]. The study revealed a wide range of SDN-specific threats, for which no countermeasure has been prescribed yet. Some of the threats discovered are inherently tied to principles of SDN design which include controllers becoming potential central attack targets; the authors suggested key factors and constraints of a secure SDN architecture.

By applying the STRIDE threat model, they came up with a generic SDN concepts as a basis for the design of a secure SDN architecture.

[4] presented the development and qualitative evaluation of a functional and secure tele-clinical diagnostic system for effective delivery of medical services to patient in a geographically dispersed academic environment. Their results showed that the combination of concepts of Software engineering, Telemedicine, and Information Security in this study can help healthcare professionals improve trust, efficiency, enhanced work productivity and improved

operational speed of medical health delivery significantly by ensuring the safety of patient data and service reliability in tele-consultation. However, the password based authentication used for user authentication is not sufficient enough to guarantee access control of the system. The delay experienced during tele-consultation can be exploited by eavesdroppers whose exploit will be detected too late as a result.

Data Security and Threat Modeling for Smart City Infrastructure was investigated by [15]. Their approach involves taking hundreds of features from the architecture of systems and network topology, operating systems, database schemas, security policies, encryption techniques, business operations, and corporate data into consideration by looking at smart city architecture, firewalls and malware protection programs. The vulnerability assessment stage is a repeated process with many threat analysis life cycles. The algorithm was used to compute threat factor and normalizes it based on the initial data collected. A lower threat factor means the smart city systems would be hacked at lower risk. Their approach also used defense in depth and strategies for threat mitigations, and provides recommendations.

Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD Model was studied by [16]. They proposed a novel fuzzy approach using DREAD model for computing the level of risk that assures a more efficient evaluation of imprecise concepts. Thus providing the ability to include subjectivity and uncertainty in the course of ranking risk. They presented a case study emphasize and compare the proposed approach with the existing method one using Matlab.

[17] used a STRIDE threat model to identify all possible threats to telehealth systems. System assets, threat agents, adverse actions, threats and their effects alongside their various countermeasures. These threats were examined and a list of possible mitigation techniques were presented as countermeasures for insider threats. A threat model using Microsoft threat modeling tool 2014 was established to enhance the system security in terms of protecting healthcare information from security threats which include patient data disclosure and/or unauthorized access or modification by attackers. In rating the threats discovered in the investigations, the authors did not use any systematic computations or methodology in rating the threats as high, medium or low risk to the systems. This can be achieved using a DREAD risk-assessment model for computer security threats which provides a mnemonic for risk rating security threats using five categories to obtain a hybrid threat model whose threats are properly rated.

III. METHODOLOGY FOR MODELING THREAT IN ELECTRONIC HEALTH SYSTEMS

The modeling of threats in computer systems software has been widely used and involves a number of techniques. The essential process involved has been described in [6] and discussed in [3]. To model threats for the eHealth system, three essential steps are followed as described below:

- Identify Assets of the EHS
- Identify Access points
- Identify threats
- Rate the identified threats

A. Identifying Assets

An asset is any valuable component of a system that may be owned by the system and holds an interest for attackers. Attackers here refer to persons or processes that constitute a threat to the asset from within or outside the system or environment where it is being used. Recognizing assets is the most important step in threat modeling. This is because assets are primary targets of threat. For an EHS, the assets include the system itself, the various hardware and software components that allow it to function and the various actors that interact with the system. Figure one shows the actors (assets) that interact with the EHS. Assets are not limited to just the actors, the server, computer systems, mobile devices, network, cabling, power source, and power outlets are all assets of the EHS and should be accorded the same level of consideration when identifying assets in this phase.

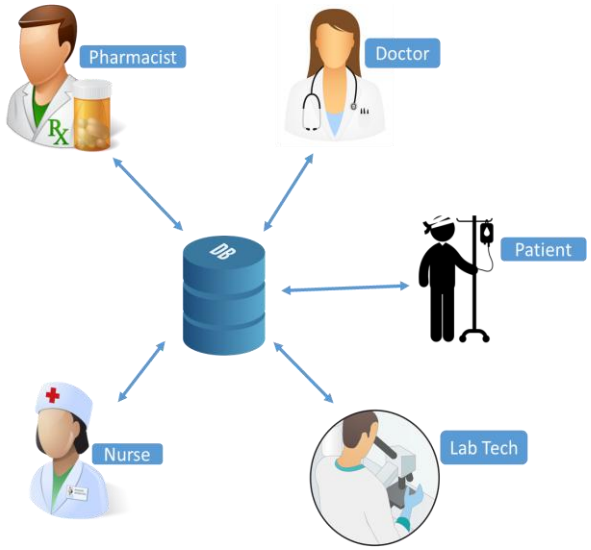

Figure 1. Various actors interraction with EHS Database in single site scenario.

Figure 1 shows various actors who interact with the EHS to generate different types of data that is peculiar to their departments in a healthcare facility and a patient which are store in the database. The nurses on the front desk may create a patient profile for a patient on his first visit to the health care facility with his biodata and a unit identification is generated for the patient, a doctor records his diagnosis of the patient in the database along with recommendations as regards test to be conducted on the patient at the lab. The lab technician accesses the data and conducts the test and records findings into the database. The doctor accesses this data and makes prescriptions and recommendations to admit the patient or not. The pharmacist fills the prescription and the patient leaves the health care facility. If the system is accessible by the patient over the internet, he/she may login to book appointments for another visit.

B. Identifying Access points

Access points are the various interfaces threat posing attackers may use to interface with the system to obtain unauthorized privileges to assets. Hardware ports, login screens and user interfaces, open sockets, RPC interfaces and

configuration files are examples of access points on systems. Trust boundaries determination is related to access points in the system. Upon recognizing an access points, it is essential to define trust boundaries for the access point in the system. A trust boundary refers to a boundary over which different levels of trust exist. Trust levels stipulate the amount of trust necessary to access a given part of the system. For instance, a network may form a trust boundary, as anyone may gain access to the internet through the network, but not everyone on the internet should have access to the enterprise network. Connected to trust boundaries are trust levels. Trust levels stipulate the amount of trust required to access a portion of the system.

C. Identifying Threats to the EHS

Threats may result from the activities of legitimate users of a system (insiders) who are authenticated and authorized to use the services provided by the system or unauthorized users (outsiders). Threats are often born out of weaknesses in design, implementation or configuration and is now a course for concern to all who use information management systems for their various operations. All the information gathered from detection of access points will help to detect potential threats from the access points. The goal of an adversary, their capabilities and what the risk they pose are all referred to as threats. Threats are identified by a systematic review of assets and access point to create a premise as regards breaches of the CIA of the information system which in this case is the EHS. This is done using the STRIDE model created by Microsoft for considering threats to system security and provides a mnemonic for security threats classification in six different categories described below;

- **Spoofing –** Spoofing is a situation where a person or program masquerades successfully as an unsuspecting individual to gain an unauthorized access to otherwise information by falsifying data to get illegitimate advantage.
- **Tampering** – Tampering involves changing data for the purpose of mounting an attack. This may be done by an insider or an outsider. The insider who has access to certain privileged information may change them for malicious reasons or in order to gain access to information which they do not have clearance to view officially.
- **Repudiation** – If a system user, legitimate or otherwise, is capable of denying the claim that they have carried out a certain transaction detected in the system, the system is said to be lacking the non-repudiation characteristic of a secured system. Without any adequate logging of activities on systems and auditing, it is difficult to prove that a repudiation attacks has occurred.
- **Information disclosure** – Information disclosure attacks occur when confidential information is leaked to a user who does not have authorization to access such information.
- **Denial of service** This attack occurs when there is an attempt to make a machine, a system or resource offered by a network unavailable to those who are intended to use it This could be a temporarily or indefinitely suspension or interruption of services of a host connected to an enterprise network or the Internet.
- **Elevation of privilege** – Elevation of privileges occurs if a user finds a way to gain access beyond that which there are legitimately unauthorized to access and begin to use resources and services reserved for higher privilege users.

D. Rating Identified Threats

A simple High, Medium, or Low scale may be used to rate threats. A threat rated as High, means that threat poses a significant amount of risk to the application and needs to be resolved by implementing appropriate counter measures as soon as possible. If a threat is identified as Medium, it also need to be addressed, but with less urgency as will be required for a High-risk threat. Low risk threats may be ignored depending on how much cost and effort it may require to address the threat.

The problem posed by a simplistic rating system as described above is that risk assessment team members or security experts usually will not agree on ratings. To resolve this, a systematic way of determining what the impact of a security threat really entails is required. Microsoft's DREAD model is used to calculate risk. By using the DREAD model, you arrive at the risk rating for a given threat by asking the following questions:

- Damage Potential – How extensive is the damage potential if a vulnerability is exploited?
- Reproducibility – How easy is it to repeat the attack?
- Exploitability – How easy is it to launch an attack?
- Affected Users – As a rough percentage, how many users are potentially affected by the attack?
- Discoverability – How effortless is it to find the vulnerability?

DREAD is an acronym formed from the first letter of each class enumerated above. The risks are still rated as High medium and low risks but over the DREAD scheme with corresponding values of 3, 2, 1 respectively and zero (0) if the threat possesses no risk at all. Table 1 shows the threat rating scheme.

After threats are identified using the STRIDE model, there are rated using DREAD risk assessment model which is a categorizing scheme to qualify, analyze and prioritize the quantity of risk presented by assessed threat. The DREAD algorithm, shown below, is used to compute a risk value, which is an average of all five categories.

Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

In Figure 2, a threat model for an EHS is illustrated. It shows the database as a central asset that all the users interact with by using the various interfaces available to them via a browser based. Using the DREAD model, we ranked the threats in terms of the damage potential, reproducibility of the attack, how easy it is for malicious individuals to exploit, affected users and how discoverable the loop hole in the system is. The threats in the model above

are discussed in the order of increasing potential for discoverability, exploitation and reproducibility. The threat with the easiest discoverability is that inherent in the patients' usage of the system. A Doctors login access details may be spoofed by eavesdroppers or by simple social engineering practices such as shoulder surfing, Pretexting, Phishing etc. When this happens, access may fall into an unauthorized person who can then view privileged or private information of the all patients and with the right technical knowledge, the cracker may even prevent other users from login into the system. This access may also be disclosed by the doctors themselves to friends or family members. This threat is the most discoverable, exploited and repeated several usages of the exploit if counter measures are not implemented. The next point of threat is from nurse's interaction with the EHS. The threats posed are that of repudiation, information disclosure, privilege elevation and tampering. The ability of a system user to perform an action, malicious or otherwise and successfully deny their involvement in such action which may include but not limited to information disclosure to unauthorized personnel or tampering with patient's medical records is referred to as repudiation. The same scenario will apply to all the actors interacting with the EHS. However, in order of increasing discoverability, the last being the hardest to discover but most threatening, it proceeds from the Nurses station to the Doctors access level, the pharmacists access level, the lab technician and the database where all data created and used by all the actors are store and retrieve for decision making purposes. Here, (the Database) the inherent threat is denial of service (DoS) where the attacker attempts to exhaust the resources available to the network, application or service so that real users cannot gain access and tampering for malicious exploits.

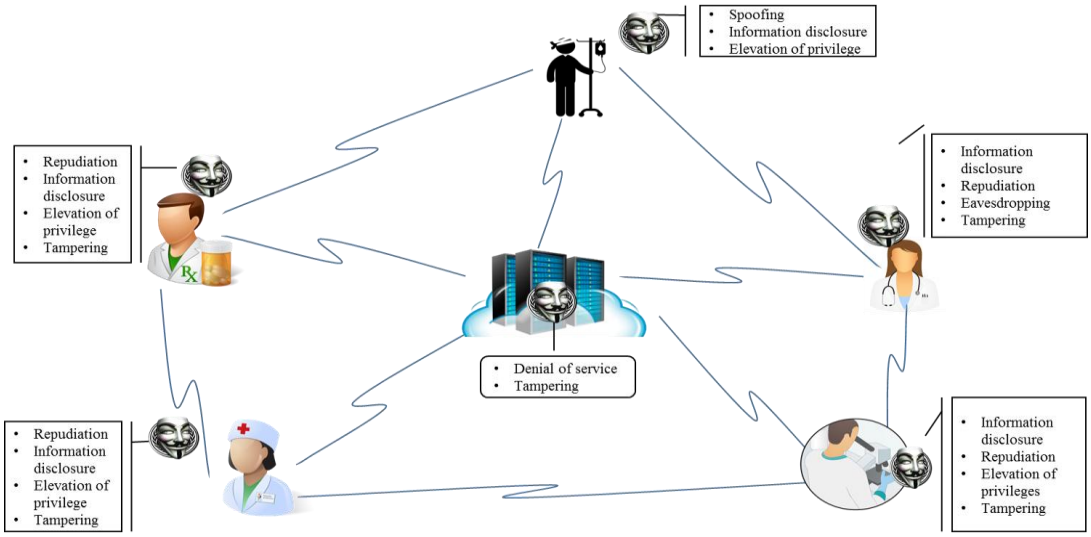

Figure 2. Threat model for an EHS

TABLE I. DREAD THREAT RATING SCHEME [9]

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

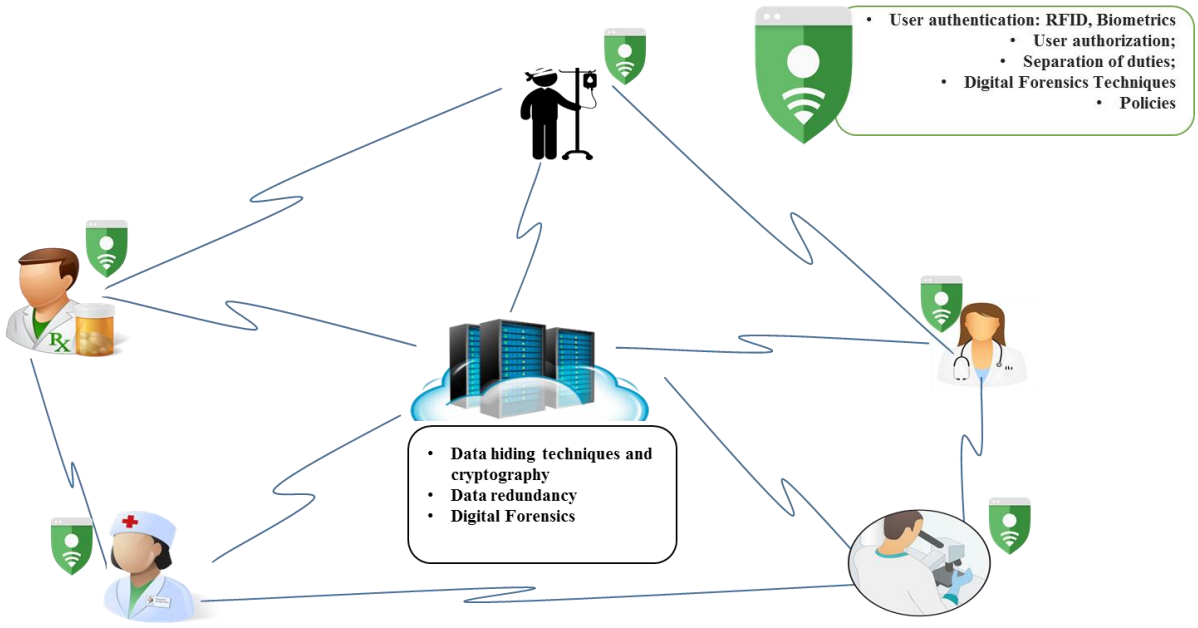

Figure 3. Countermeasures to identified threats in the model

The counter measures required to mitigate the threats in the model in Figure 2 are highlighted in Figure 4. The countermeasures are classified into two groups. The first group of countermeasures is best suited to the actors that use the database asset while the other set of countermeasure apply to the database itself.

IV. RESULTS AND DISCUSSIONS

Figure 2 is the threats identified in an EHS using the STRIDE threats modelling tool.

All possible threats associated with user authentication and authorization using login credentials that may allow illegitimate users gain unauthorized access to the system are defined. The major sources of such threats include losing, sharing or theft of user identity, login credentials, and authentication of patient medical or communication devices. Sharing of sensitive user access credentials may result in misuse, altering of sensitive patient data, or private information divulgence, among others.

Potential damage posed by this threats are computed using the DREAD risk rating scheme in Table 1 and subsequently categorized as low (0 – 6), medium (7 – 11) or high (12 – 15), according to the impact the threat possesses to the EHS as calculated in Table 2. For example, if a patient's login credentials fall into the hand of an attacker due to theft or sharing; the impact would be low, because the vulnerability is only present for a single patient; but if on the hand a health care professional say an administrator of the system with a high trust boundary fall into the hand of a malicious user, the impact will be very high, because the impact of such a vulnerability may affect more than one patient, possibly all the patients records on the server may be compromised or configurations altered by the assailant. Since authentication of communicating device is very essential, when a patient's communication device wants to exchange information with the patient's medical device, the two devices must authenticate each other, and ensure that they are what/who they claim to be. Similarly, when the patient's communication device intends to send or receive data from the EHS, both devices must carry out mutual authentication to ensure trust between the receiving and sending devices as well as the data being transmitted.

To assign risk rating values to the threats as shown on Table 2 each category of rating in the DREAD risk model was used to evaluate each threat on Figure 2. The threats generated are accompanied with description for which a DREAD value is computed on the premise discussed from the cause and effect of the threat. The process was iterated for a couple of the threats to obtain ratings which were used to compute the risk value.

Risk_DREAD may now be calculated from Table 2 as:

Risk_DREAD = (43+43+41+48+42) / 5 = 217/5 = 43.4

V. COUNTERMEASURES TO IDENTIFIED THREATS IN THE MODEL

A. *User Authentication – RFID or BIOMETRICS*

User authentication plays a vital role in many applications that require user interaction with data and services. Several remote user authentication schemes and their enhancements was proposed by [4] to improve the security flaws in other schemes. The security of the traditional identity-based remote user authentication schemes is based on the passwords. Simple passwords however, are easy to break by simple dictionary search attacks. To resolve such problem, biometric-based user authentication schemes are better alternatives since such authentications are more secure and reliable than traditional password-based authentication schemes. The advantages of using biometric keys (for example palm-prints, faces, fingerprints, irises, hand geometry, etc.) are:

- Biometric keys cannot be lost
- Biometric keys cannot be forgotten.
- Biometric keys are exceptionally hard to forge.
- Biometric keys are difficult to copy or share.

TABLE II. TABLE SHOWING EHS THREATS RATED WITH DREAD

Threat	D	R	E	A	D	Total	Rating
Personnel identity spoofing	3	2	2	3	3	13	High
Loss or stolen of personnel communication device	3	1	3	3	3	13	High
Denial of service to patients	3	2	2	3	3	13	High
Unauthorized access	3	2	2	3	2	12	High
Personnel Identity misuse	3	2	2	3	2	12	High
Data tampering by Personnel	3	2	2	3	2	12	High
Weak access control	3	2	2	3	2	12	High
Denial of service to personnel	3	2	1	3	3	12	High
Illegitimate access to administrative interfaces	3	2	2	3	2	12	High
Unauthorized disclosure	3	3	3	2	1	12	High
Spoofing of EHS source server	3	2	1	3	2	11	Medium
Loss or stolen of patient's communication device	2	1	3	1	3	10	Medium
Personnel information repudiation	0	3	2	3	2	10	Medium
Elevation using impersonation	2	2	2	2	2	10	Medium
Log files tampering	3	2	1	2	2	10	High
Insufficient auditing	0	3	1	3	2	9	Medium
Patient Identity misuse	1	3	2	1	1	8	Medium
Data tampering by patients	0	3	3	1	1	8	Medium
Patient information repudiation	0	3	2	1	2	8	Medium
sharing or Loss of patient identity	1	0	2	1	1	5	Low
Patient identity spoofing	1	1	1	1	1	5	Low

- Biometric keys cannot be easily guessed as compared to low-entropy passwords.
- Biometrics of someone's not easy to break than others.

If biometric authentication is implemented on the EHS, the following attacks will be prevented.

- Withstand masquerade attacks where an adversary may try to masquerade as a legitimate user to communicate with a valid system or masquerade as a valid system in order to communicate with legal users.
- Withstand replay attacks that occur when an attacker tries to hold up the messages between two communicating parties and then impersonate other legal party to replay the fake messages for further deceptions.
- Withstand man-in-the-middle attacks where attacker intercept the messages during transmissions and can change or delete or modify the contents of the messages delivered to the intended recipients.

A couple of remote user authentication schemes that use smart cards have been proposed in the literatures [3] [6]. A self-certified user authentication scheme for next generation wireless network, which relies on the public-key cryptosystem was proposed as an efficient biometric-based remote user authentication scheme using smart card in [13]. If the flaws highlighted in [7] are resolved, it will serve as a means for a secure user authentication system with RFID enabled smart cards for any system and not just on an EHS.

B. User Authorisation and Seperation of Duties

This can be achieved through programming logic to ensure that each user group only access the parts of the systems that they are authorized to access and use the functions that are specific to that user group without any access to tasks and functions that are for other user groups. Separation of duties is a classic security method to manage conflict of interest, the appearance of conflict of interest, and fraud as shown in Figure 4. It restricts as much as possible the amount of power held by any one individual by ensuring that each user group only performs read and write operations on data that pertains to it. It puts a barrier in place to prevent fraud that may be perpetrated by adversaries. Fraud is more likely to occurs when there is a collusion in the functions performed by a user group with the functions of a different user group.

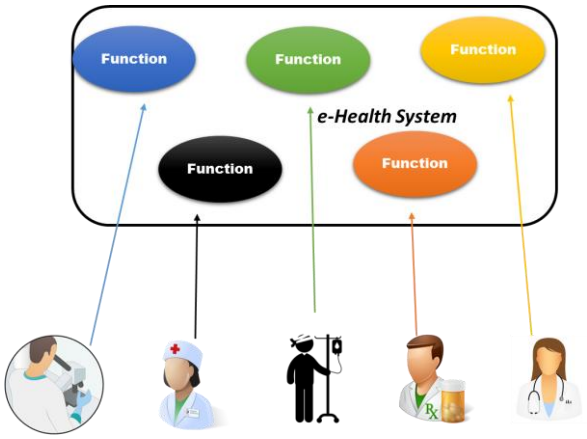

Figure 4. Seperation of Duties

VI. CONCLUSION

This paper proposes a threat model for an Electronic health systems (EHS) that captures the possible attacks that may be carried out against an EHS. The STRIDE threat model was used to identify potential threats which were then ranked based on the security risk posed using a DREAD threat-risk ranking model. Possible countermeasures to authentication and authorization control threats on the system were discussed. Our future research work will focus on Design and development of scalable security controls and

countermeasures to the various threats identified in this paper. We will also explore the digital forensic techniques that could be used at different parts of the system when a successful attack is carried out and policies that need to be put in place to ensure that the occurrences of attack are minimized.

REFERENCES

[1] O. Stella and M. E. Herselman, "E-health in Rural Areas: Case of Developing Countries," *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering,* vol. Vol:2, No:4, 2008, p. 7, 2008.

[2] D. J. Brailer, "Economic Perspectives on Health Information Technology," *Business Economics,* vol. 40, p. 8, 2005.

[3] S. Alshehri, S. Mishra, and R. Raj, "Insider threat mitigation and access control in healthcare systems," 2013.

[4] O. M. Olaniyi, T. A. Folorunso, A. Omotosho, and A. Israel, "Securing Digitized Campus Clinical Healthcare Delivery System," presented at the 1st International Conference on Applied Information Technology, 2015.

[5] V. Garg and J. Brewer, "Telemedicine security: a systematic review," *Journal of diabetes science and technology,* vol. 5, pp. 768-777, 2011.

[6] F. Swiderski and W. Snyder. Threat Modeling [Online].

[7] M. Hardy, "Beyond Continuous Monitoring: Threat Modeling for Real-time Response," *SANS Institute,* 2012.

[8] S. S. Techtarget, "Definition of Threat Modeling," ed, 2016.

[9] Microsoft. (2003, 8/11). *Chapter 3 - Threat Modeling*. Available: https://msdn.microsoft.com/en-us/library/ff648644.aspx

[10] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, 2005, pp. 1-8.

[11] S. Kumar and B. K. Tripathi, "Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach," *Procedia Technology*, vol. 24, pp. 1268-1275, // 2016.

[12] O. A. Adebisi, D. A. Oladosu, O. A. Busari, and Y. V. Oyewola, "Design and Implementation of Hospital Management System," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 5, 2015.

[13] P. Anand, J. Ryoo, H. Kim, and E. Kim, "Threat Assessment in the Cloud Environment: A Quantitative Approach for Security Pattern Selection," in *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, 2016, p. 5.

[14] F. Ruffy, W. Hommel, and F. von Eye, "A STRIDE-based Security Architecture for Software-Defined Networking," *ICN 2016*, p. 107, 2016.

[15] P. Wang, A. Ali, and W. Kelly, "Data security and threat modeling for smart city infrastructure," in *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, 2015, pp. 1-6.

[16] A. Singhal and H. Banati, "Fuzzy Logic Approach for Threat Prioritization in Agile Security Framework using DREAD Model," *arXiv preprint arXiv:1312.6836*, 2013.

[17] M. Abomhara, M. Gerdes, and G. M. Køien, "A STRIDE-Based Threat Model for Telehealth Systems," *Norsk informasjonssikkerhetskonferanse (NISK)*, vol. 8, pp. 82-96, 2015.