Tiako P.F. (ed) *Automated Systems, Data, and Sustainable Computing*. Chronicle of Computing. OkIP.
 https://doi.org/10.55432/978-1-6692-0001-7_6

Detecting and Preventing Approach for Electronic medical records in E-Health

Lynda Sellami[a], Khaled Sellami[b], Piere F. Tiako[c], Djilali Idoughi[b]
[a]*Computer Science Department, University of Bejaia, Algeria*
[b]*LMA Laboratory, Faculty of Ecxact Sciences, University of Bejaia, Algeria*
[c]*Center for IT Research and Development, Tiako University, Oklahoma, USA*

ABSTRACT

E-Health is designed to support the activities of patients, including the transmission of their medical history between healthcare professionals, the renewal or adaptation of prescriptions remotely, and the transmission of their test results online. Ensuring the security and confidentiality of patient information is a crucial point, hence the need to protect patient medical data and ensure their well-being at the same time. In this article, we propose to develop an IDS for the protection of patient medical data. Our work aims to overcome intrusion problems by developing an intrusion detection system based on legitimate healthcare professional authentication, signals and prevents intruders from breaking in. The proposed model protects patients and ensures the security of medical resources.

Keywords: E-Healthcare Records, Security, Intrusion Detection System, Covid-

I. INTRODUCTION

E-Health facilitates patients' lives, including transmitting their medical healthcare diagnosis between healthcare professionals, renewal of remote prescriptions, and the receipt of their test results online (Thimbleby, 2013).

The e-Health allows the installation of medical equipment connected to the patient's home to provide physicians with information on the patient's condition (Eysenbach, 2009).

The development of e-Health is hampered by patients' fear of disclosing medical confidentiality and the confidentiality of their data. Therefore, it is necessary to secure personal data and healthcare records (Sellami, Tiako, & Sellami, 2018).

In this article, we propose developing an IDS for detecting and identifying altered health records in medical systems by authenticating legitimate Healthcare Professionals/patients, reporting and preventing the Healthcare Professionals/patients who provide abnormal services. The approach is applied and tested on a set of Covid-19 medical data to prove the proposed solution's effectiveness and feasibility in detecting unauthorized abnormal activities in e-healthcare environments.

The rest of the paper is organized as follows: Section II presents a state of work already done on intrusion and detection in e-healthcare environments. Section III details our proposal. We show some experimental results on a set of medical data from Covid-19 evaluating our solution in Section IV. Finally, the conclusion and perspectives are described in Section V. This Template

II. RELATED WORK

A. E-healthcare

E-Health uses the Internet and related technologies to provide health services and information at the intersection of medical informatics, public Healthcare, and business (Ziaie, 2013).

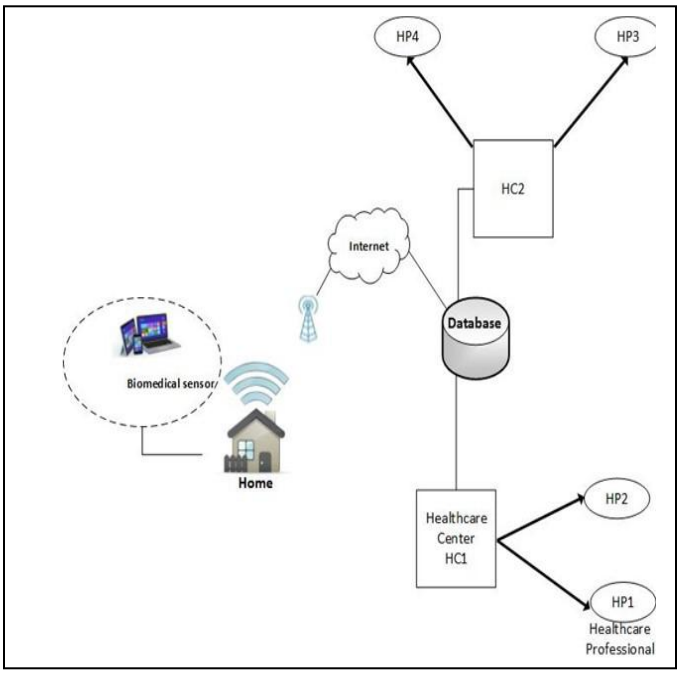

Fig. 1. General view of e-Healthcare

In Healthcare, patients' health is the primary concern of healthcare professionals within the Healthcare services (hospital) or at home.

For the care of patients at home, the home is equipped with medical sensors that react to changes in the patient's health parameters. A medical sensor collects vital parameters and medical data concerning the patient, saves them at the level of device (laptop, tablet, etc.), which transmits them to the Healthcare center where they are treated and consulted by the appropriate and authorized health professionals (Kaur, & Gupta, 2006; Al-Rimawi, Dwairej, Masadeh, Ahmad, & Al-Ananbeh, 2016).

B. Security Issues in e-Healthcare

Health systems are a vulnerable target for malicious attacks by users to undermine efficiency or deteriorate the performance of health systems (Slaymaker, Politou, Power, & Simpson, 2004). Malicious users hack hospital networks to steal personal health data as well as health possible credit canal information.

1) Medical Records Attacks: These attacks can modify information, delete critical data, or send back data messages.

2) Transmission Attacks: These attacks can modify records, intercept the communication, send additional signals to block the base station and network traffic. This attack is used for espionage.

3) Storage Attacks: These attacks can update the patient's medical records or change the configuration of the system's monitoring servers.

C. Intrusion Detection System in e-Healthcare

Connected e-Healthcare services implement Internet technologies; these services are part of the Internet network, which exposes them to the risks of attacks and intrusions. The safety of health services is an essential issue for patients and health professionals, given the importance and confidentiality of the data that these services use, share and transfer, to ensure the quality of the service provider (Barnes, 2006) and correct such possible intrusion in the system. There is a need for a proactive and comprehensive security system dedicated to controlling. The intrusion detection system (IDS) is a crucial element of any security strategy; this software tool must be implemented in every hospital, medical office, house, or other providing distance care.

An IDS can record actions on patient data. It allows monitoring and analyzing a system, detecting and correcting any anomaly, modification, or misuse of the system (Sellami, Idoughi, & Tiako, 2016; Sellami, Sellami, & Tiako, 2019).

Several IDS solutions have been implemented to address the vulnerabilities of corrects health environments. Below, we review the main IDSs that have been applied in the field of e-Healthcare:

1) IDS-based wireless device: To meet the challenges mentioned in the field of security in e-Health, Nespoli and Gomez Marmol (Nespoli, F.G Marmol, 2018) have proposed a new wireless IDS architecture. They are offered a device (sensor) of low energy consumption with characteristics of the IoT (Internet of Things). The device is called Raspberry Pi. It is used as a host system for a wireless IDS with wireless traffic monitoring, also exploiting the correlation capabilities of a SIEM platform to report detected anomalies. The sensor (device) is portable (ubiquitous aspect). It can perform its tasks using a minimal configuration by adapting its behavior to different scenarios. Its role is to protect users' communications once active (local detection) and transmit information to a remote server. The network administrator performs maintenance or emergency operations when collecting data from different sources using a SIEM platform. Incoming events are filtered, aggregated, and correlated to distinguish between malicious activity and false alarms. This process would help to identify appropriate security measures for protection.

It is interesting to collaborate with the sensors to carry out a global detection and react based on the warnings received. While waiting for the response and processing of alerts by the network administrator, the system may be attacked, which may be harmful and fatal.

2) Snort for intrusion detection: In Nenova's work (Nenova, 2015), the author proposed an IDS to protect health facilities against intrusions. The proposal uses the Snort system for network protection; the patient sensor network sends the required number of data packets to the processing units using a single connection sensor. Information collected using a tablet, laptop, or other device is processed and stored in the e-Health platform database. IDS is used to diagnose the patient and generate emergency medical care signals via the Internet. Snort is a network system based on an IP (Internet Protocol) for intrusion detection developed on an open-source basis.

When the stream is encrypted, Snort cannot start the detection process. Snort rules are stored directly in RAM at startup, which results in memory overload. RAM is emptied to handle the high flow, which allows attacks to go unnoticed (undetectable). Snort is often vulnerable to attacks by Denial of Service. It gives false alarms because of small signals

3) Collaborative IDS based on cloud services: To protect the health system against malicious attacks, Bodkhe et al. (Bodkhe, Gadkar, Mane, Pol, Tarange, & Prof-Nalawade, 2018) have developed a new collaborative method of an intrusion detection system based on the cloudlet mesh, which can effectively prevent remote data attacks (Bodkhe, Gadkar, Mane, Pol, Tarange, & Prof-Nalawade, 2018). The user provides the information on the user's body to the database. And such a database is an entry for secure sharing in a cloudlet-based system. The owner is the one accessing the information. The cloudlet system (cloud server) stores the encrypted data provided by the data owner while sharing any attacks, stopping them using the collaborative intrusions detection system method. If an authenticated health professional wants to access the data, he can decrypt the data from the cloud.

When the clients' information is transmitted to a cloudlet, the sharing of these information cause problem when harmful people use this information.

4) Anomaly-based IDS: In this solution, an anomaly-based IDS is proposed by (Itten, & Vadakkumcheril, 2016) to improve the accuracy of IDS based on existing behavior rule specifications. An Attack Detection System MCPS (Medical Physical Cyber Systems) uses multivariate correlation analysis (MCA) to accurately represent the traffic. In this system, the data attributes are collected, and the records of the protected servers and the network are monitored and analyzed to reduce IT costs. The detection process is executed in two phases when detecting an anomaly: the learning and test phases. In the learning phase, profiles are generated for each type of traffic user and stored in the data servers. In the test phase, the profiles are built for the observed traffic records. The attack detection

engine is presented during the test phase to obtain normal and abnormal data patterns.
The solution makes it possible to capture, monitor, and analyze the attributes of incoming data features and the behavior of traffic patterns and records from servers and the network. Data stored in a database becomes enormous, creating a problem with the attack detection system speed, thus allowing the attacks to go unnoticed.

D. Disadvantages of Existing System

Many of the existing systems discussed above have the following disadvantages:

- *Collaboration of the sensors* is favored for data monitoring and analysis. Alert processing is centralized at the network administrator level**,** ***exposing the network to unnoticed attacks***.
- In an e-health environment, the ***memory*** of health sensors ***is overloaded*** by monitoring and analyzing the attributes of incoming data, the behavior of traffic patterns, and server and network records.
- E-health environments are based on the principle of *information sharing*, allowing healthcare professionals to access the information they need. The problem that arises in the case of the sharing of patient' health information is its use by *harmful people*.
- The *increase in the size of the database* is due to the storage of analysis and monitoring data, which *disrupts data access* and *slows down attack detection*.
- No Trust.

III. *PROPOSED* WORK

The objective of our work is to solve the problem of detecting erroneous diagnoses in Healthcare environments. Below we propose a functional model of medical network protection using an intrusion detection system.

A. Architecture

The principle of our approach is to deal with an authorized healthcare professional accessing the medical data of a patient saved at a healthcare center. The healthcare professional must authenticate to access patient data.

B. Proposed Security Scheme

We are concerned about patient records confidentiality and security and using an IDS to detect and protect against unauthorized access.

A healthcare professional (HP) requesting access to a patient's medical information must first log in to the system. Once authenticated, all actions of the health professional are screened by the IDS. The IDS detects any abnormality or suspicious behavior of the health professional "Figure 2 ".

If an attack or intrusion is detected, further access to the information is denial, and the administrator is notified of the access attempt. The episode and information about the intruder are recorded for future investigations.

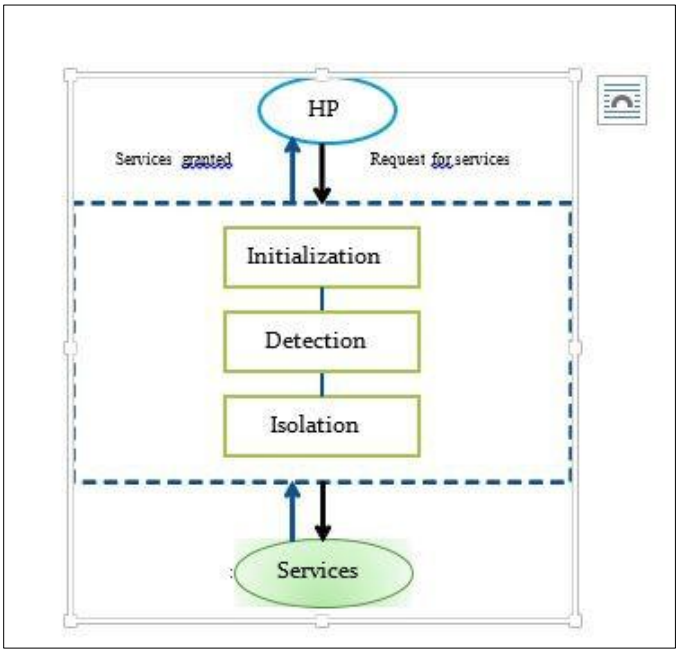

Fig. 2. IDS-Activities

C. Approach

Our IDS identifies malicious use of a computer system by comparing a predefined normal profile with the HP's actual behavior. The security scheme of our approach is broken down into three phases: the initialization phase, the detection phase, and the isolation phase. The details of these phases are described below and presented in " Figure 2 ".

1) Initialization phase: In the initialization phase, the normal profile of the healthcare professional is established based on its authentication when accessing the network. It is based on the detection of anomalies by using HP requests. When connected, a healthcare professional requests an access service to the patient's data. An authentication check is performed: which consists of the login and password of the HP's permissions and restrictions, limiting access to the information and services offered by the Healthcare network. Once the legitimacy of the healthcare professional is verified: their normal profile is built based on permissions and restrictions.
This process makes it possible to construct a vector of characteristics (attributes) V_i (0) in an initial time 0.
Let, $V_i(0) = (v_1, v_2, v_3, \ldots, v_i)^T$ the vector of attribute in initial time 0.

2) Detection phase: This phase consists essentially of two steps: (1) collecting patient behavior information to build the current behavior (CB) and (2) compare current behavior to normal profile
To detect defective vectors (behavior) in case of deviation from the normal profile implies an intrusion.

For data analysis, we apply the evaluation function that detects intrusions at the healthcare professional level of the network.

$$\sum_{i=1}^{n} \left| vi(0) - vi(k) \right| \quad (1)$$

V_i (k) is defective if the calculated projection distance of the characteristic vectors V_i (k) and V_i (0) is greater than 0.

$$\begin{cases} D(Vi(k), Vi(0)) = 0 : \text{Normal} \\ D(Vi(k), Vi(0)) \neq 0 : \text{Anomalies} \end{cases} \quad (2)$$

This calculation allows detecting any intrusion and its source (node that caused the attack).

3) Isolation phase: In case of intrusion detection, the isolation consists of: (1) cut all connections with the offending Healthcare professional; (2) remove the faulted Healthcare professional from the network; (3) keep track of attack.

IV. EXPERIMENTAL RESULTS

To better exemplify our approach and evaluate the detection results, we use a set of medical data from patients suspected of Covid-19.

A Healthcare professional uses his Personal Computer (PC) to work and access Healthcare network services and information of patients, which requires an authentication and access control mechanism to establish the healthcare professional's normal profile. The actual behavior of the HP is collected to detect any deviation (change) in the normal behavior of the Healthcare professional.

To develop the function of our IDS model, we have made several intrusions. We used a set of medical data from patients and a vector of Healthcare professionals authorized.

For testing purposes, bad packets with illegitimate data packets are sent to the simulated system. The bad packets contain unauthorized Healthcare professionals.

The results of the analysis and detection are shown in Table 1; we note that bad packets (by default) are effectively identified and eliminated. Intrusion attacks are generated to develop the functioning of our IDS model in a healthcare network., We sent bad packets and good packets to test the simulated system. The results of the analysis and detection are shown in Table 1; we note that bad packets (by default) are effectively identified and eliminated. In "Table 1", we note that the detection rate (ID) and the rate of normal behavior (NB) are very high.

Our IDS model detects new attacks from inside and outside the network, which affect proper network functioning.

TABLE I. DETECTION RESULTS

Normal data size (KB)	Intrusion data size (KB)	Normal behavior	Intrusion detection
50	40	50	100%
150	80	150	100%
200	100	200	99,83%

V. CONCLUSION

E-Health provides home health devices and applications to make life easier for patients and healthcare personnel. This flexibility and ease of use expose the E-Health system to many Internet attacks and anomalies. It is imperative to develop traffic monitoring methods for the detection of attacks in e-Health systems and networks.

The main objective of this work is to ensure the safety of the E-Health system. Our approach helps control the security of patient medical data against misuse. This process involves looking for anomalies that could lead to possible attacks and taking action against such attacks.

The proposed model ensures the overall security of health records in the medical environment, thus avoiding errors in the diagnosis and treatment of patients.

REFERENCE

Clark, T., Woodley, R., & De Halas, D. (1962). Gas-Graphite Systems. In R. Nightingale (Eds.), *Nuclear Graphite* (pp. 15-26). Academic Press, New York.

Thimbleby, H. (2013). Technology and the Future of Healthcare. J Public Health. 1; 2(3): e28. Published online 2013 Dec 1. doi: 10.4081/jphr.2013.e28.

Eysenbach. (2009). e-healh, http://www.jmir.org/2001/2/e20/. (Access November 2019).

Sellami, L., Tiako, P.F., & Sellami. T. (2018). Genetic Algorithm for Intrusion Detection System in Pervasive Medical Resource. International conference on operation research, Bussels, Belgium.

Ziaie. N. (2013). e-Health Security Issues and Solutions, Master of Science Thesis, University of Gothenburg. Göteborg. Sweden.

Kaur, G., Gupta. & E-health, N. (2016). A New Perspective on Global Health. Journal of Evolution & Technology. ISSN 1541-0099. 15(1).

Al-Rimawi, R., Dwairej, D., Masadeh, A., & Ahmad E, M. (2016). Al-Ananbeh. E-health Concept Development and Maturity in Literature. Journal of Health, Medicine and Nursing. ISSN 2422-8419. An International Peer-reviewed Journal. Vol.29

Slaymaker, M., Politou, E., Power, D., & Simpson, A. (2004). e-Health security issues: the e-DiaMoND perspective. Proceedings of UK e-Science All Hands Meeting.

Barnes. J. (2006). Intrusion Detection Systems in Hospitals: What, Why, and Where. Unpublished manuscript. East Carolina University. Greenville. North Carolina. Retrieved from http://citeseerx. ist. psu. edu/viewdoc/download.

Sellami, L., Idoughi, D., & Tiako, P.F. (2016). Detection of New Attacks on Ubiquitous Services in Cloud Computing and Against Measure. Advanced Science Letters 22 (10), 3168-3172, Canada.

Sellami, L., Sellami, K., & Tiako, PF. (2018). Efficient Management of Security for Supporting Intrusion Detection in Ubiquitous and Pervasive Environments. Procedia Computer Science 155, 402-409, Canada 2019.

Nespoli, P., & Marmol. F.G. (2018). e-Health Wireless IDS with SIEM integration, IEEE Wireless Communication and Networking Conference (WCNC).

Nenova, M.V. (2015). Investigation of intrusion detection and intrusion prevention systems in eHealth hospital network. E+E. 3-4.

Bodkhe, S., Gadkar, A., Mane, S., Pol, P., Tarange, J., & Prof-Nalawade, T.B. (2018). Medical Data Sharing For Protection and Intrusion Avoidance in Cloudlet. International Research Journal of Engineering and Technology (IRJET). e-ISSN: 2395-0056, Vol: 05 Issue: 10.

Itten, A., & Vadakkumcheril, G.T. 2016). Enhanced Intrusion Detection System in Medical Cyber Physical Systems Using Multivariate Correlation Analysis. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE). ISSN: 0976-1353, Vol: 22 Issue: 4.