Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Ensuring Electronic Health Record Cyber-Security through an Hybrid Intrusion Detection System

Mario Sicuranza, Giovanni Paragliola

RT-ICAR-NA-2020-01 ***Data:*** **maggio 2020**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) – Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: *www.na.icar.cnr.it*

Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Ensuring Electronic Health Record Cyber-Security through an Hybrid Intrusion Detection System

Mario Sicuranza, Giovanni Paragliola

Rapporto Tecnico N: **RT-ICAR-NA-2020-01** ***Data:*** **maggio 2020**

Ensuring Electronic Health Record Cyber-Security through an Hybrid Intrusion Detection System

Mario Sicuranza, Giovanni Paragliola

Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche
Via Pietro Castellino, 111 – 80131 Napoli, Italia

E-mail: {mario.sicuranza, giovanni.paragliola}@icar.cnr.it

Abstract

Ensuring cyber-security of Electronic Health Record (EHR) is a challenging task due to complexity and heterogeneity of IT systems supporting business processes. Several solutions have been proposed to protect this infrastructure but they mainly are focused on the detection of unauthorized accesses. In this paper we propose an Intrusion Detection System (IDS) architecture designed to address cyber-security in a EHR. The proposed IDS is based on three main components: a misuse detection module that allows to detect well-know attacks; an anomaly detection module that is able to detect zero-day attack; an expert system aims to resolve possible conflicts between misuse and anomaly modules. In cooperation with experts of the domain, we identified and simulated three real cyber-attacks that may affects a EHR infrastructure. Experimental results shown the effectiveness of IDS proposed.

Keywords: Misuse Detection; Anomaly Detection; Intrusion Detection System; Electronic Health Record.

1 Introduzione

Nowadays, several utilities constitute very important assets for the modern society (e.g., telecommunications, energy supply, dams, health care). This is because many essential services were developed which use these infrastructures to support citizens' activities. For this purpose, U.S. Department of Homeland Security [27] has classified some infrastructures as Critical i.e., it has identified the assets, systems, networks, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. In the last years the adoption of IT systems within Critical Infrastructures has increased. Thus, the introduction of IT networks, monitoring and control systems has improved the infrastructure management, but it has also increased the number of cyber-attacks that these utilities are exposed to. Among the types of CI, in this work we focus on a specific kind of ones, the Electronic Health Record (EHR). The EHR is a health system for collection and management of patient's clinical data in order to guarantee both medical research and continuity of care. The clinical documents and data are provided by many types of health entities such as care-centers, hospitals, laboratories, and etc, where each one of them may be located at different places such as districts or cities. These information may be collected, shared and used only by authorized users by means of EHR system's facilities. However, some misuse cases could be exploited by attackers or malicious users in order to compromise EHR system and the privacy of users e.g. by accessing to private documents. In terms of types of attacks to EHRs, in this work we face the problem related to unauthorized accesses in EHRs system. Techniques which address these kinds of attacks can be classified in Misuse and Anomaly detection techniques. Misuse detection techniques allow to detect well-known attacks signatures with high detection rate but they are not able to detect zero-day attacks. In particular, an alarm is generated if a previously described attack signature is detected. Anomaly detection techniques allow to detect zero-day attacks by modeling the normal user or system behavior. Alarms are raised when significant deviations from the model built are detected. However, there are cases in which events that deviate from the system profile are not necessarily

malicious [9]. In this paper, to address the intrusion detection issue we propose an hybrid Intrusion Detection System (IDS) architecture that uses both misuse and anomaly detection techniques to detect both zero-day attacks and well-known attacks against EHRs. In order to improve detection accuracy, anomaly detection is performed by using a voting system which combines the outputs provided by different techniques. The architecture also provides mitigation of the disadvantages of anomaly and misuse detection (e.g. high false positives and incapability of detecting previously described attacks e.g. through signatures). This is obtained through an Expert System, which has a detailed knowledge of the specific domain considered and so it can: i) improve the detection accuracy of cyber attacks; ii) solve conicts when they are raised. In particular, a conflict is raised when the outputs provided by misuse and anomaly detection techniques do not agree e.g., the anomaly detection technique detects a possible attack whereas the misuse detection technique detects that it is not an attack. The proposed architecture has been validated within a prototype health system (i.e., EHR system, a particular kind of Critical Infrastructure). Experimental results show the effectiveness of the proposed solution. The remainder of the paper is detailed as follows. In Section 2 the commonly used detection techniques for Cyber-attacks are detailed; in Section 3 the conceptual architecture is described; in Sections 4 and 5, we describe the dataset used for the validation and the preliminary results. Finally, in Section 6 concluding remarks and future works are discussed.

2 Related Work

There are a lot of challenges that must be addressed to ensure cyber-security of a critical infrastructure as EHR. Moreover, Privacy Rights Clearinghouse stated that more than 260 million \records" of all types have been breached in the U.S. since January 2005 [11] [1]. IDS represents an enabling technology that can be used to detect security breaches within monitored infrastructure. Several works are proposed which use this technology to ensure the cyber-security of a generic critical infrastructure. A classic classification of IDSs defines two basic approaches: Misuse detection strategies and Anomaly detection strategies. We refer to Misuse Detection strategy in the case when an IDS looks for events or sets of events that match a predefined signature of a known attack; instead we refer to Anomaly Detection strategy in the case when the IDS identifies intrusions as unusual behavior that differs from the normal behavior of the monitored system.

2.1 Misuse Detection Techniques

Misuse Detection Techniques can be divided in two types: signature-based and Rule-based. In signature-based IDSs, events are monitored and matched against a database of known attack signatures to detect intrusions. Rule-based systems use a set of if-then implication rules to characterize cyber-attacks. In this kind of IDSs, events are monitored and then coded in facts and/or rules that are later used by an inference engine to draw conclusions and claim if an attack is occurring or not. In [14] the authors propose a novel intrusion detection framework for securing Wireless Sensor Networks (WSNs) from routing attacks. IDSs based on state transition techniques define a finite state machine that models the system's evolution over the input; authors do not consider the limited resources available of each node of WSN. Rule-based approach is a simple model that can be adapted for any problem. It is suitable both when the problem can be written by using “if-then" rules and when there are not too many rules that can be difficult to be maintained. In [12] the authors propose an hybrid IDS designed by taking into account the limited resources available on nodes of a

WSN. In particular, a threshold-based technique is used to detect anomalies within messages analyzed by each node. An alert is generated when a security threshold is overcome. In [20], the authors model computer penetrations as a series of state changes that lead from an initial secure state to a target compromised state. The state transition analysis is a rule-based approach for penetration identification. Decision tree based approaches are easy to understand and they can be easily translated in rules to be implemented. In [28] the authors discuss about a multi-strategy pruning algorithm to improve decision tree based IDS. In [19] the authors propose an IDS based on three feed-forward multilayer perceptron neural networks with back-propagation learning and voting scheme. The voting scheme performs a combination of best outputs of the neural networks. Neural networks are quite simple to implement; also, they can adapt to unknown situations and they are able to model complex functions.

2.2 Anomaly Detection Techniques

Anomaly Detection Techniques can be divided in several types. Classification based techniques define a model from a dataset of labeled instances, so called training; the learned model is then used to classify test instances in different classes. The simplest classification model entails a binary classification as normal, abnormal. Statistical based techniques produce a statistical model from given data; such model embodies the normal behavior of the monitored system i.e. when not under attack. After the model is built, incoming instances are tested in order to check if the current instance belongs to the model or not. When an instance does not match the model, it is marked as an anomaly. In rule-based approaches, a knowledge base is defined which describes the normal system behavior, so the anomaly evaluation is performed by comparing this predefined normal behavior with the current activities of the system. Profile based techniques are grounded in the definition of a profile or description of the system that we need to monitor. The profile describes the activities of the system by means of attributes. In [13], the authors propose a novel approach to detect anomalous records in categorical datasets through Bayesian Networks. In particular, the authors use the formulation of suspicious coincidence proposed by Barlow [7]. The goal is to detect unusual shipments among all imports into the country. In [25] the authors proposed EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment, which defines a statistical profile-based anomaly detection module. This technique is focused on characterizing the past behavior in order to detect significant deviations. In [9] authors provide a survey about the use of machine learning and soft computing methodologies to perform intrusion detection. In particular, unsupervised, supervised, statistical and ensemble techniques are analyzed and discussed. In [29] the authors propose a credit card fraud detection model. In particular, the proposed algorithm calculates the distances between each data object and its neighbors. Thus a matrix is created where the element $d_{i;j}$ represents the distance between two data objects. Then the sum of row elements Pi is performed.
Finally, an out-lier is identified if Pi overcomes an established threshold. This approach can be useful against a fake data injection attack. In [18], the authors present an approach based on data mining that supports automatic signature discovery in a network-based IDS. The proposed approach is based on Apriori algorithm [5]. A critical infrastructure, of high interest is the EHR. In fact, it represents a critical asset in the modern society and thus it must be protected to avoid disasters and economic damages. Several works are proposed to ensure cyber-security of this infrastructure and they can be classified in two main categories: the first category contains the systems designed to detect only inappropriate accesses to EHR i.e. these systems analyze access logs with different techniques in order to discover unauthorized accesses; the second category contains the solutions proposed to improve the resilience of the EHR from any type of misuse e.g. attacks, faults and failures. In fact, the goal of these systems is to ensure availability of business services. Thus, global constraints on the system are established and a non-stop monitoring activities ensures that these constraints are

satisfied. The authors of [10] propose a community-based anomaly detection model called CADS. In particular, the proposed system detects relationships between users by observing the access logs. To predict cyber-attacks from malicious users, CADS calculates deviation of users based on their nearest neighbors' networks. Two datasets are used to validate the proposed approach and a comparison performed with Principal Component Analysis (PCA) and K-Nearest Neighbors (KNN) algorithms. In [24] authors propose an approach inspired by collaborative filtering to create a more _ne-grained model for detecting inappropriate accesses to EHR. Collaborative filtering is a popular strategy, where the implicit characteristics of users and items are detected only historical preferences, and they are used to predict preferences for every pair (user, item). The authors compare the proposed collaborative filtering model with three supervised learning methods: linear regression, logistic regression, and SVM with linear kernel. In [6] authors discuss about a threat modeling methodology called attack tree. Such methodology allows to analyze the threats affecting EHR system. An attack tree is a conceptual tree where each node represents a single attack and it is activated when the children nodes (sub-attacks) are true. The purpose of the authors is to identify possible attacks against EHR and to propose suitable countermeasures. In [23] [22] authors propose a new system called System Health and Intrusion Monitoring (SHIM) to perform a continue monitoring and assesment of the health and security of a distributed system. In particular, the authors do not model a specific attack but they define the constraints on the system (i.e. specific constraints are defined for protocols, network services and other). An intrusion, fault or error occurs if these constraints are violated. In [8] the authors propose a system called Monitoring Access Pattern phase 1 (MAP1) to detect inappropriate access to EHR. Two methods are analyzed to detect suspicious activities and they are logistic regression and support vector machine. In [2] authors discuss about the optimization of classifiers in the previous work [8]. In particular, they use filtering techniques in order to detect rare events and to reduce the number of false positives. Our purpose is to improve the cyber-security of EHR by designing a new IDS customized for this infrastructure. In particular, the proposed IDS architecture is general and can be adapted to different scenarios. Also starting from the knowledge of the domain experts we identified some cyber-attacks that affect the EHR and we proposed and validated techniques to ensure cyber-security of the considered infrastructure.

3 Intrusion Detection System for EHR

The figure 1 shows an overview of EHR system in which different local EHR are meshed to realize an abstraction of unique EHR. The EHR system allows to make patient's clinical information safe and available only to authorized users, in order to guarantee confidentiality, quality, and efficiency of the medical cares. Nowadays patients' mobility is sensibly increasing as much as patients receive medical treatments in areas that may be different from where they live on. This situation has increased the need of integration among healthcare systems placed on different local domains.
The integration of heterogeneous health systems also raises difficulties in addressing of security issues as well as the assuring of requirements such as confidential, intrusion identification and attacks detection. In Figure 2 we show the proposed conceptual architecture to ensure cyber-security of EHR. Each component of the IT infrastructure provides logs which provide information as system identification, operations performed, requested user's roles, firewall status. Logs analysis is useful to perform security analysis and to avoid security breaches. Logs generated from any source within the monitored infrastructure are gathered by different software agents. Software agents perform a preliminary security analysis and send their output (events) to Misuse and Anomaly Detection modules. Both the modules are equipped with a corresponding Knowledge Base, which is used to

perform a more complex and complete analysis then a single agent. Both modules independently analyze the events generated by the agents in order to discover suspicious activities. If the outputs provided by both modules disagree then the Expert System is invoked. The Expert System can be a human expert which resolves the conflict, decides if an attack is occurring or not and updates the knowledge base of the modules (if necessary).

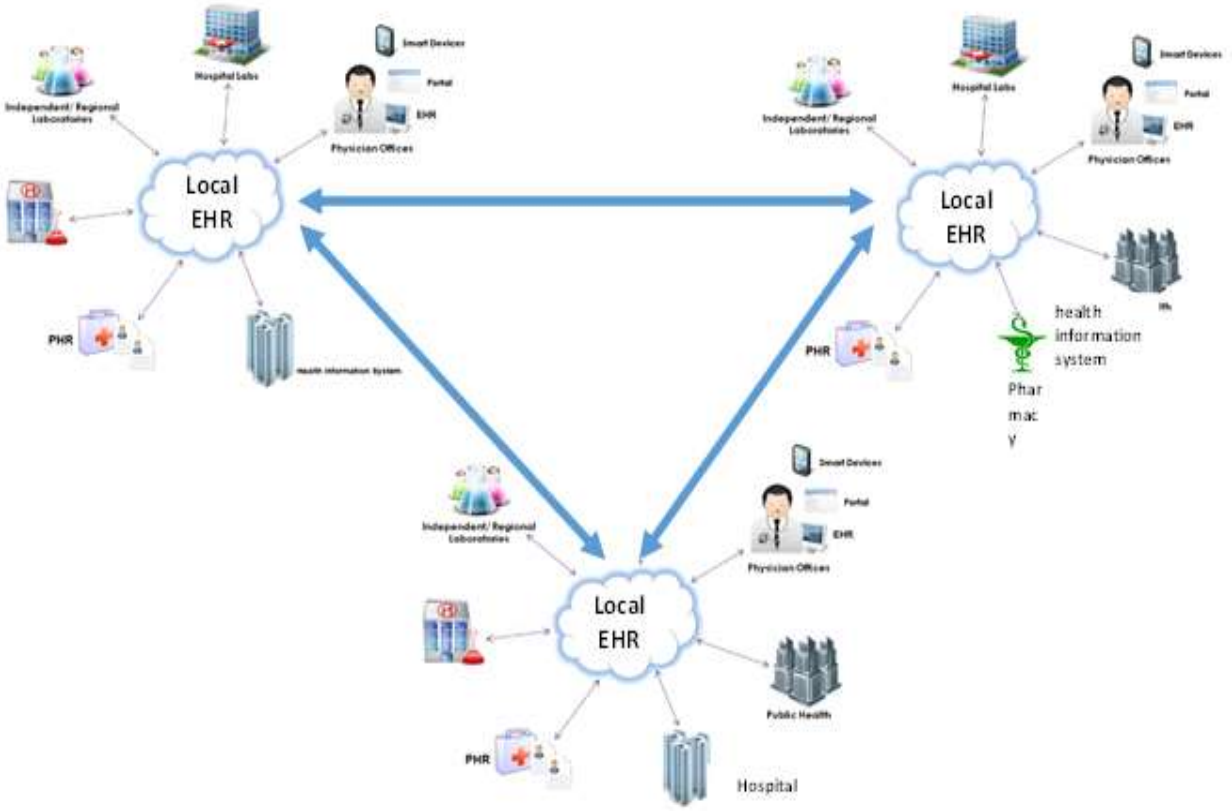


Figure 1 Overview of the EHR Architecture

Finally, if an attack occurs then the Expert System stores raised alarms/anomalies into a *Resilient Storage*. The Resilient Storage is a facility designed to be tolerant to intrusions and faults [3]. The components of the proposed architecture are detailed in the following.

3.1 Agents

Agents are software modules deployed within the monitored IT infrastructure i.e. the EHR. In particular, agents must be designed to gather and to process a huge amount of logs and eventually to handle even traffic peaks which can cause overload on a specific agent. These requirements can be satisfied through a federated agents model which dynamically optimizes allocation of resources and available agents. Each data source generates logs in a specific format chosen by the corresponding producer, this makes the logs analysis harder when data are heterogeneous. To overcome this limitation, each agent performs a normalization process i.e. all gathered logs are translated in events with a common format and a specific semantic. Finally, each agent uses its own local knowledge to perform fine-grained security analysis.

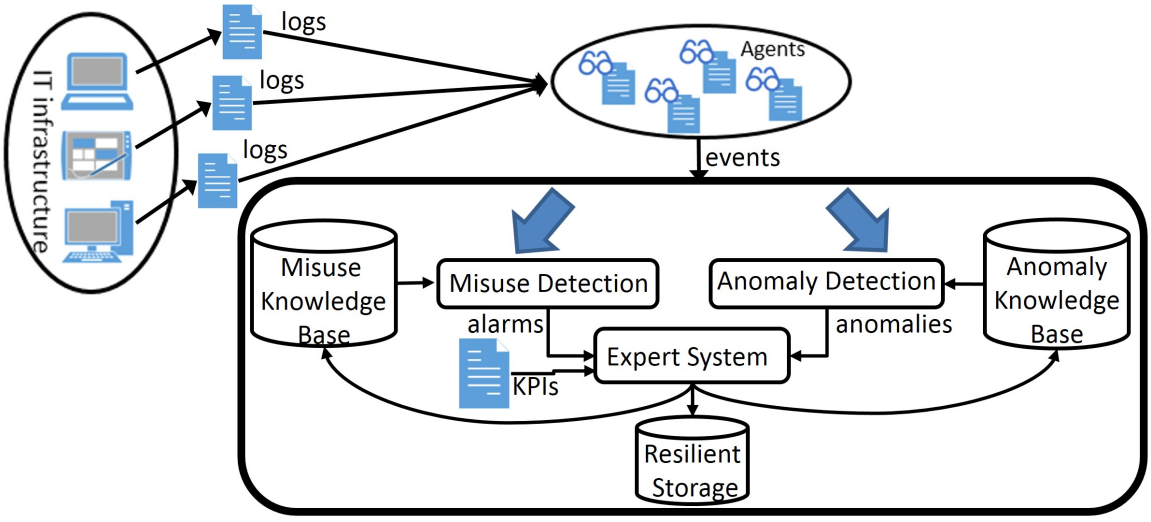


Figure 2 Architecture proposed to protect the EHR from cyber-attacks

3.2 Misuse and Anomaly Detection

The generated events are sent both to the Misuse and the Anomaly Detection module for security analysis. Misuse Detection module allows to detect well-known attacks, e.g. widely known attacks that can be described through signatures. The advantage of this kind of approach is that well-known attacks are accurately identified and their signatures are stored in misuse knowledge base. In this paper, the Misuse Detection module uses the well-known rule-based approach to perform security analysis. The specific rule-based technique used is the classification using association rules [4]. The disadvantage of Misuse Detection module is that an attack cannot be detected successfully if a description of the attack signature is not available. To overcome this limitation, we propose to support Misuse Detection module with an Anomaly Detection module. Anomaly Detection is a complementary approach to misuse detection that allows to discover new or unknown attacks. Anomaly Detection is based on the concept of the baseline. In particular, a baseline describes the normal behavior of the monitored phenomenon. A known disadvantage of anomaly detection is that it may generate many false positives. To overcome this limitation a vote-based approach has been defined. The Anomaly Detection module sends the same events to different classifiers-based sub-modules that use different data analysis techniques. In particular, three classifiers are presented in this paper, and they are: decision tree, neural network and k-means. Few solutions are known in the literature in the designing of IDS solutions for a specific critical infrastructure i.e. the EHR. Thus, we investigated the usage of these techniques well-known in literature to ensure cyber- security of this new scenario. The outputs of those classifiers are provided to a voting system that allows to reduce the false positives generated by each single classifier. The decision about the occurrence of an attack is taken by combining the results of the single classifiers.

3.2.1 Misuse Detection

The proposed Misuse Detection module is implemented by an association-rules-based approach [4]. Let $I=\{i_1, i_2, \ldots, i_m\}$ be a set of m attributes called items. Let $Z = \{t_1, t_2, \ldots, t_m\}$ be a set of tuples called dataset. In particular, a rule describes a correlation between items of tuples within the dataset. An intrusion is identified when a rule is fired. These rules describe the frequency of relation between items within dataset. Two measures are used to evaluate the quality of an association rule, and they are: Support and Confidence. Support indicates the percentage of data within the dataset that show the correlation; confidence can be interpreted as an estimate of the probability P (Y X), where Y and X are two items within the dataset. An association rule is considered strong if both Support and

Confidence of the rule overcome minimum thresholds defined by experts of considered domain.

3.2.2 Anomaly Detection

The architecture of Anomaly Detection module is based on the combination of three different classifiers and a voting system as shown in Figure 3.

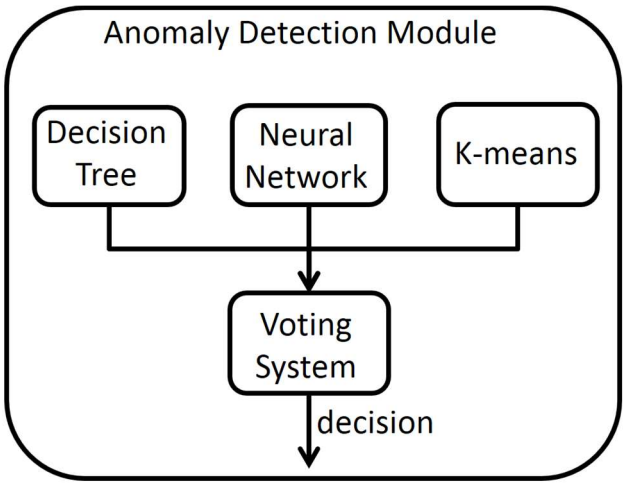


Figure 3 - Architecture of Anomaly Detection module

In this work the considered classifiers are: decision tree, neural network and k-means.
Decision tree and neural network are supervised techniques whereas k-means is an unsupervised technique. Supervised techniques require training data to infer a function. Training data are based on a set of training examples. Each example is a pair of input data and an output value called label. The function describes the relation between training examples. Each example is a pair of input data and an output value called label. The function describes the relation between inputs and the provided labels. The function inferred is used to map new incoming examples. Unsupervised techniques do not require labels and they try to find a structure within unlabeled training data. Each of the three classifiers output a "vote" (attack/no attack), for each event. The vote indicates if the event is related to an attack or not. The outputs of the classifiers are sent to the voting system whose purpose is to provide the final decision if the event analyzed is related to a cyber-attack. The goal of voting system is improving the detection accuracy of each single classifier.

3.3 Expert System

The Expert System uses a set of high-level policies defined by an expert of the specific domain in order to extract a set of Key Performance Indicators (KPIs) from them; KPIs represent the attributes that must be monitored to enforce policies.
The Expert System has three information sources: i) alarms raised by the Misuse Detection module; ii) anomalies raised by the Anomaly Detection module; iii) KPIs extracted from policies. Table 1 describes the way the expert system processes the alarms/anomalies.
If both Misuse and Anomaly Detection modules do not raise any alarm/anomaly (first row in the table), the Expert System does not perform any action. If the Misuse Detection module raises an alarm and the Anomaly Detection module does not detect any anomaly (second row in the table) or vice-versa (third row in the table), then a conflict is generated and the Expert System is invoked.
In this case the Expert System has to resolve the conflict in order to decide if an attack in occurring or not. Thus, it evaluates the impact of alarm/anomaly identified through KPI previously established. As consequence of its evaluation, the Expert System will update the knowledge base of the Anomaly or Misuse Detection module. Furthermore, the Expert System stores the alarm related to the attack

detected within the Resilient Storage. The last case of Table 1, i.e. when both modules generate an alarm/anomaly, is referred to the case when the attack is recognized and so this alarm/anomaly is stored in Resilient Storage.

Misuse Detection	Anomaly Detection	Effect
0	0	None
1	0	Update the knowledge base of the anomaly or misuse module
0	1	Update the knowledge base of the anomaly or misuse module
1	1	Stores alarms/anomalies in Resilient Storage

Table 1 - The behavior of the Expert System with reference to outputs of Anomaly and(or) Misuse Detection modules

4 Experimentation of the Misuse and Anomaly Detection Modules

In this section we are going to describe the preliminary results related to the evaluation of the proposed architecture. We have tested the system on a prototype of an Italian EHR system.
In detail, we will present

- The data-set used for the training and testing of the intrusion detector modules.
- The preliminary results of the classification

4.1 Dataset

The data-set was defined by means of agents distributed within EHR system. Events generated by agents represent the required operations on the system by the user. The data-set is composed by a set of tuples; each one of them is made of a set of simple attributes:

- *Source Domain*, it is coded by the standard ISO [15] , possible values for this attribute can be {IT-65, IT-77, IT-78, IT-72, IT-45, IT-36, IT-62, IT- 42, IT-25, IT-57, IT-67, IT-21, IT-75, IT-88, IT-82, IT-52, IT-55, IT-23, IT-34, IT-32, IT-BZ, IT-TN}; it is worth noting that these codes represent the identification of the local health systems.
- *Operation*, it defines the operation required by the user, possible values are: {Search, Retrive, Update, Insert}
- *Destination Domain*, it defines the requested domain by the current operation; the possible values are the same of the source domain;
- *Date*, it defines the request time; it is coded using the standard ISO 8601, (the adopted format is YYYYMMDDhhmmss) [17]
- *Outcome*, the outcome is the result of the operation; the possible values can be {ok, user not identified, user not authorized, wrong system}
- *Patient ID*, it is the code that allows the identification of the patient that requires a specific document.
- *User ID*, it is the identification of the requesting user
- *Document Type*, it represents the type of requested document; the possible values are coded by means of the standard LOINC [16]
- *Role*, it defines the role of the requesting user in the system, possible values can be: GP (General Practitioner); Pharmacist (Pharmacist); Physician (Physician Pathology); Specialist (Specialist Physician); Patient (Patient)}

In addition to the simple attributes presented above, other features have been added within the data-set. These features allow to detect different attacks in a simpler and quicker way. They are composed attributes, which are defined by a pre-processing stage over sets of tuples. The composed attributes are:

- *Npat20*, it represents the number of patient's documents requested by a specific user in the last 20 minutes
- *Ndoc20*, it defines the number of documents retrieved by a specific user in the last 20 minutes
- *Nop5*, it defines the number of times that a specific operation is done for a specific type of document in the last 5 minutes
- *LivdocRec*, it defines the correlation level between the retrieved type of documents for a specific user. The correlation among the documents has been defined with the support of health domain process experts; the correlation values can assume integer values equal or up to 1, where one states for the maximum value of correlation

Figure 4 shows an example of tuple.

Source Domain	Operation	Destination Domain	Data	Outcome	Patient ID	User ID	Document Type	Role	Npat20	Ndoc20	Nop5	LivdocRec
IT-45	Ricerca	IT-45	20140301-084522	ok	OXXXXX00X00X000X	UXXXXX00X00X000X	34133-9	MMG	1	0	0	0

Figure 4 - Example of a tuple of the data-set

5 Results

In this section we are going to present the preliminary results of the anomaly and misuse modules of the proposed architecture. Both have been modeled with KNIME [21], a graphic tool that implements WEKA [26], a Java-based library for the implementation of artificial algorithms.

5.1 Misuse Detection

The misuse detector has been modeled by means of the Rule Engine components of Knime 5. It allows to implement the association rules approach. We have defined and tested three kinds of rules for the detection of attacks on the system. These rules have been suggested by an expert of the domain who has suggested us how to take in consideration the attacks.
The tested attacks are:

- *GP Attack* - A specific general practitioner user, searches and retrieves more then 9 documents about more than 4 different patients in the last 20 minutes.
- *Consent Attack* - More than 30 consents (that is a type of document) are modified in a 5 minutes time range in some domain
- *Uncorrelation Documents Attacks*, a user retrieves more than 30 uncorrelated documents in a 20 minute time range

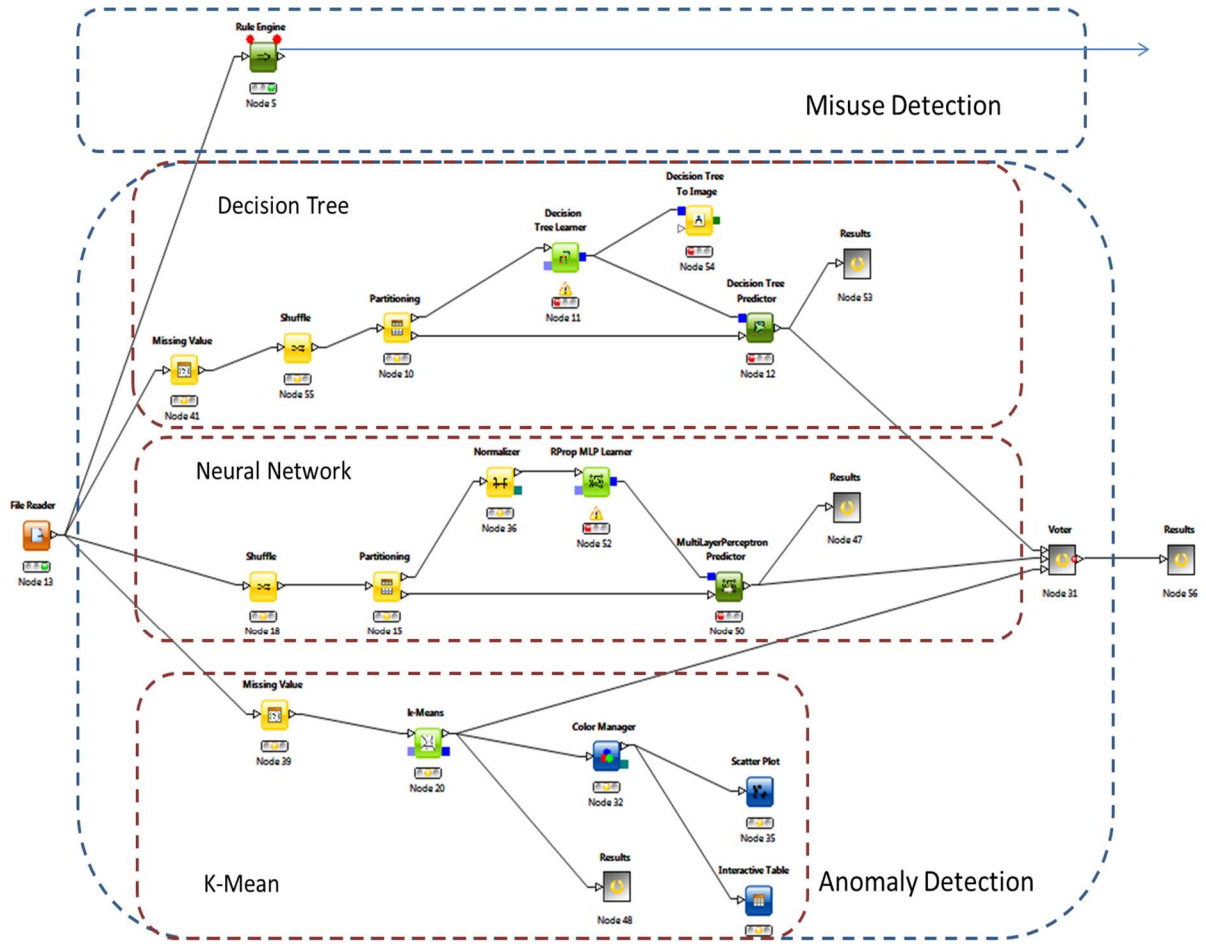


Figure 5 - Overview of the detecting modules in Knime

The Figure 6 shows the rules coded in Knime for the detection of the attacks.
The Figure 7 presents a sub-set of the results of the classification performed by the misuse module. It is possible to note the outputs of the module for the three kinds of attacks. The tuples undetected as attack are labeled with the symbol ”?”. The identification code of both the user and the patient have been blinded for privacy reasons.

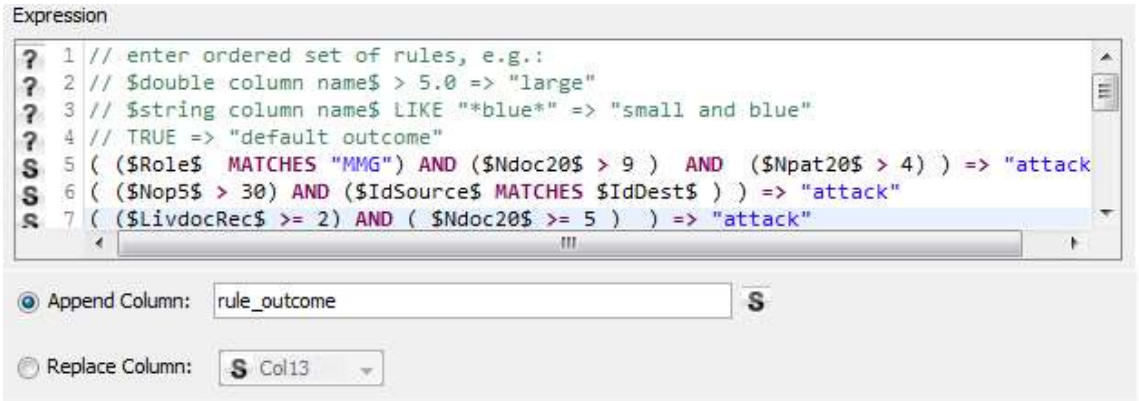
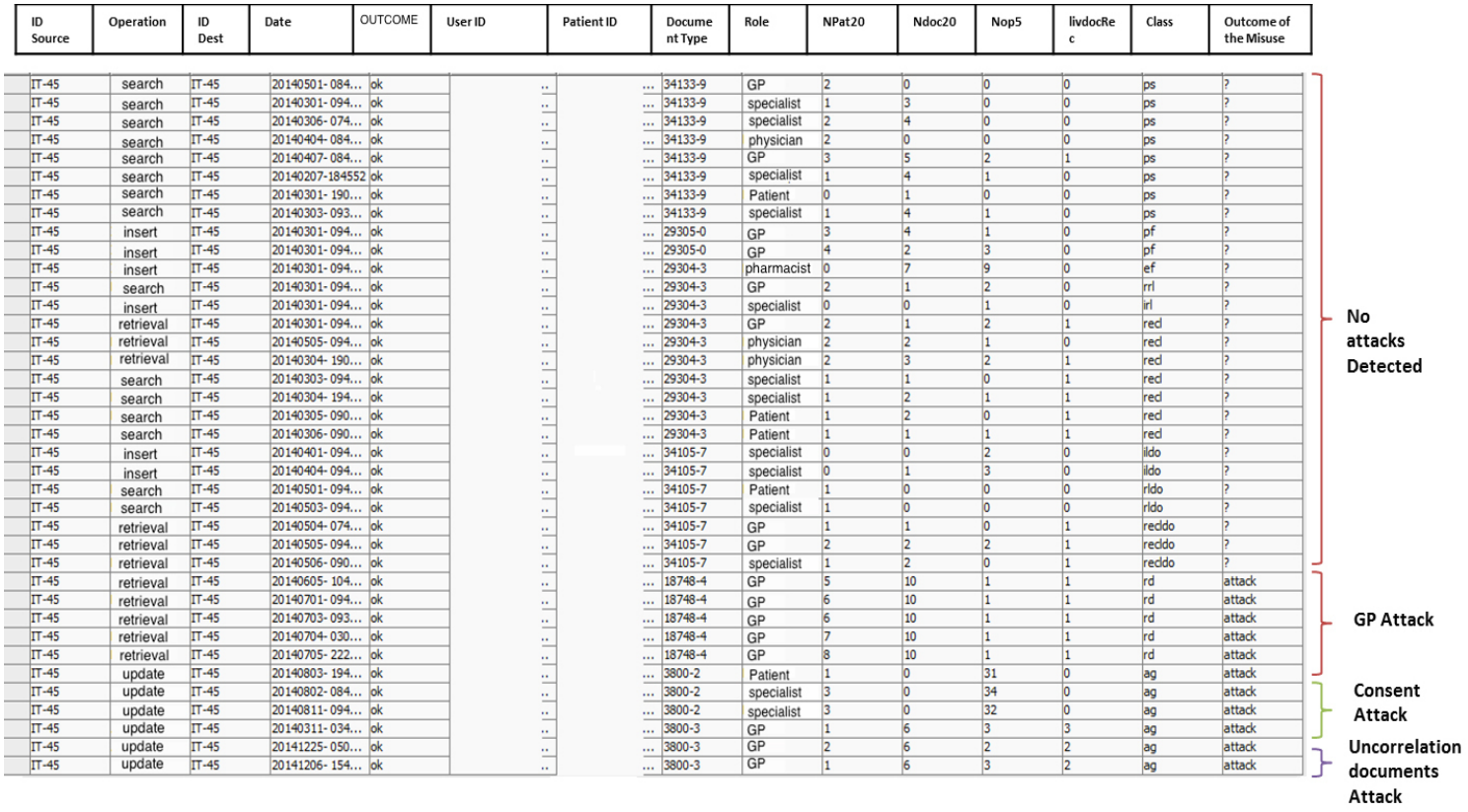


Figure 6 - misuse detection module based on association rules



ID Source	Operation	ID Dest	Date	OUTCOME	User ID	Patient ID	Document Type	Role	NPat20	Ndoc20	Nop5	livdocRec	Class	Outcome of the Misuse
IT-45	search	IT-45	20140501-084...	ok	..	...	34133-9	GP	2	0	0	0	ps	?
IT-45	search	IT-45	20140301-094...	ok	..	...	34133-9	specialist	1	3	0	0	ps	?
IT-45	search	IT-45	20140306-074...	ok	..	...	34133-9	specialist	2	4	0	0	ps	?
IT-45	search	IT-45	20140404-084...	ok	..	...	34133-9	physician	2	0	0	0	ps	?
IT-45	search	IT-45	20140407-084...	ok	..	...	34133-9	GP	3	5	2	1	ps	?
IT-45	search	IT-45	20140207-184552	ok	..	...	34133-9	specialist	1	4	1	0	ps	?
IT-45	search	IT-45	20140301-190...	ok	..	...	34133-9	Patient	0	1	0	0	ps	?
IT-45	search	IT-45	20140303-093...	ok	..	...	34133-9	specialist	1	4	1	0	ps	?
IT-45	insert	IT-45	20140301-094...	ok	..	...	29305-0	GP	3	4	1	0	pf	?
IT-45	insert	IT-45	20140301-094...	ok	..	...	29305-0	GP	4	2	3	0	pf	?
IT-45	insert	IT-45	20140301-094...	ok	..	...	29304-3	pharmacist	0	7	9	0	ef	?
IT-45	search	IT-45	20140301-094...	ok	..	...	29304-3	GP	2	1	2	0	rrl	?
IT-45	insert	IT-45	20140301-094...	ok	..	...	29304-3	specialist	0	0	1	0	irl	?
IT-45	retrieval	IT-45	20140301-094...	ok	..	...	29304-3	GP	2	1	2	1	red	?
IT-45	retrieval	IT-45	20140505-094...	ok	..	...	29304-3	physician	2	2	1	0	red	?
IT-45	retrieval	IT-45	20140304-190...	ok	..	...	29304-3	physician	2	3	2	1	red	?
IT-45	search	IT-45	20140303-094...	ok	..	...	29304-3	specialist	1	1	0	1	red	?
IT-45	search	IT-45	20140304-194...	ok	..	...	29304-3	specialist	1	2	1	1	red	?
IT-45	search	IT-45	20140305-090...	ok	..	...	29304-3	Patient	1	2	0	1	red	?
IT-45	search	IT-45	20140306-090...	ok	..	...	29304-3	Patient	1	1	1	1	red	?
IT-45	insert	IT-45	20140401-094...	ok	..	...	34105-7	specialist	0	0	2	0	ildo	?
IT-45	insert	IT-45	20140404-094...	ok	..	...	34105-7	specialist	0	1	3	0	ildo	?
IT-45	search	IT-45	20140501-094...	ok	..	...	34105-7	Patient	1	0	0	0	rldo	?
IT-45	search	IT-45	20140503-094...	ok	..	...	34105-7	specialist	1	0	0	0	rldo	?
IT-45	retrieval	IT-45	20140504-074...	ok	..	...	34105-7	GP	1	1	0	1	reddo	?
IT-45	retrieval	IT-45	20140505-094...	ok	..	...	34105-7	GP	2	2	2	1	reddo	?
IT-45	retrieval	IT-45	20140506-090...	ok	..	...	34105-7	specialist	1	2	0	1	reddo	?
IT-45	retrieval	IT-45	20140605-104...	ok	..	...	18748-4	GP	5	10	1	1	rd	attack
IT-45	retrieval	IT-45	20140701-094...	ok	..	...	18748-4	GP	6	10	1	1	rd	attack
IT-45	retrieval	IT-45	20140703-093...	ok	..	...	18748-4	GP	6	10	1	1	rd	attack
IT-45	retrieval	IT-45	20140704-030...	ok	..	...	18748-4	GP	7	10	1	1	rd	attack
IT-45	retrieval	IT-45	20140705-222...	ok	..	...	18748-4	GP	8	10	1	1	rd	attack
IT-45	update	IT-45	20140803-194...	ok	..	...	3800-2	Patient	1	0	31	0	ag	attack
IT-45	update	IT-45	20140802-084...	ok	..	...	3800-2	specialist	3	0	34	0	ag	attack
IT-45	update	IT-45	20140811-094...	ok	..	...	3800-2	specialist	3	0	32	0	ag	attack
IT-45	update	IT-45	20140311-034...	ok	..	...	3800-3	GP	1	6	3	3	ag	attack
IT-45	update	IT-45	20141225-050...	ok	..	...	3800-3	GP	2	6	2	2	ag	attack
IT-45	update	IT-45	20141206-154...	ok	..	...	3800-3	GP	1	6	3	2	ag	attack

Figure 7 - Results of the misuse detection module

5.2 Anomaly Detection

The anomaly detection system is made by a voting approach among three different detection techniques, respectively decision tree, neural networks and k-means.
Figure 5 shows the components that have been used to realize both the detectors and voter module.
The three detection modules have been defined as binary classifiers, so their exit can be a binary value {*anomalous* or *normal*}.
The voter evaluates the three outcomes of the classifiers and adopts a majority voting approach in order to state if an anomaly is happening or not.
The figures 8 and 9 show:

- The confusion matrix of the three classifiers 9
- The accuracy matrix of both the three classifiers and the voter 8

ACCURACY TABLE OF THE DECISION TREE

Row ID	TruePositives	FalsePositives	TrueNegatives	FalseNegatives	Recall	Precision	Sensitivity	Specifity	F-meas...
norm	740	50	190	0	1	0.937	1	0.792	0.967
attack	190	0	740	50	0.792	1	0.792	1	0.884
Overall	?	?	?	?	?	?	?	?	?

ACCURACY TABLE OF THE NEURAL NETWORKS

Row ID	TruePositives	FalsePositives	TrueNegatives	FalseNegatives	Recall	Precision	Sensitivity	Specifity	F-meas...
norm	715	72	155	12	0.983	0.909	0.983	0.683	0.945
attack	155	12	715	72	0.683	0.928	0.683	0.983	0.787
Overall	?	?	?	?	?	?	?	?	?

ACCURACY TABLE OF THE K-MEANS

Row ID	TruePositives	FalsePositives	TrueNegatives	FalseNegatives	Recall	Precision	Sensitivity	Specifity	F-meas...
norm	900	45	198	12	0,987	0,952	0,987	0,815	0,969
attack	198	12	900	45	0,815	0,943	0,815	0,987	0,874
Overall	?	?	?	?	?	?	?	?	?

ACCURACY TABLE POST VOTING

Row ID	TruePositives	FalsePositives	TrueNegatives	FalseNegatives	Recall	Precision	Sensitivity	Specifity	F-meas...
norm	912	28	202	1	0,999	0,970	0,999	0,878	0,984
attack	202	1	912	28	0,878	0,995	0,878	0,999	0,933
Overall	?	?	?	?	?	?	?	?	?

Figure 8 Results of the anomaly detection approach

6 Conclusion

In this work the authors propose an hybrid IDS architecture to ensure cyber-security of a specific critical infrastructure i.e. EHR. Proposed architecture analyzes events generated by different agents deployed within EHR in order to discover security breaches. Security analysis is performed by the misuse and anomaly detection modules. Misuse detection allows to detect well-know attack signatures whereas anomaly detection allows to detect the zero-day attacks. Anomaly detection generates several false positives so we used three different classfiers that analyze the same events and a voting system in order to improve the detection accuracy of the anomaly detection module. Also, an expert system module has the purpose to solve eventual conflicts raised between the presence/absence of attacks as estimated by the misuse detection module and the anomaly detection voting system. In order to validate the proposed architecture, a dataset was created by monitoring the Italian EHR system. Misuse and anomaly detection modules were tested by considering 3 different attacks affecting EHR systems. The results show the effectiveness of the proposed approach.

Confusion Matrix of the Decision Tree

	Norm	Attack
Norm	740	0
Attack	50	190

Confusion Matrix of the Neural Networks

	Norm	Attack
Norm	715	12
Attack	72	155

Confusion Matrix of the k-means

	Norm	Attacks
Cluster1	900	12
Cluster2	45	198

Figure 9 Confusion Matrix of the anomaly detection module

7 References

[1] Symantec: Security and Privacy for Healthcare Providers. http://eval.symantec.com/ mktginfo/enterprise/white_papers/b-security_and_privacy_for_healthcare_WP_ 20934020.en-us.pdf.

[2] Anomaly and Signature Filtering Improve Classifier Performance For Detection Of Suspicious Access To EHRs., volume 2011, 2011 2011.

[3] M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, and L. Romano. A resilient architecture for forensic storage of events in critical infrastructures. In High-Assurance Systems Engineering (HASE), 2012 IEEE 14th International Symposium on, pages 48–55, Oct 2012.

[4] Rakesh Agrawal, Tomasz Imielin´ski, and Arun Swami. Mining association rules between sets of items in large databases. In Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data, SIGMOD '93, pages 207–216, New York, NY, USA, 1993. ACM.

[5] Rakesh Agrawal and Ramakrishnan Srikant. Fast algorithms for mining association rules in large databases. In Proceedings of the 20th International Conference on Very Large Data Bases, VLDB '94, pages 487–499, San Francisco, CA, USA, 1994. Morgan Kaufmann Publishers Inc.

[6] Ahmad Almulhem. Threat modeling for electronic health record systems. Journal of Medical Systems, 36(5):2921–2926, 2012.

[7] H. B. Barlow. Unsupervised learning. chapter Unsupervised Learning, pages 1–17. Bradford Company, Scituate, MA, USA, 1999.

[8] Aziz A Boxwala, Jihoon Kim, Janice M Grillo, and Lucila Ohno-Machado. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. Journal of the American Medical Informatics Association, 18(4):498–505, 2011.

[9] Francesco Camastra, Angelo Ciaramella, and Antonino Staiano. Machine learning and soft computing for ict security: an overview of current trends. Journal of Ambient Intelligence and Humanized Computing, 4(2):235–247, 2013.

[10] You Chen and Bradley Malin. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. In Proceedings of the First ACM Conference on Data and Application Security and Privacy, CODASPY '11, pages 63–74, New York, NY, USA, 2011. ACM.

[11] Privacy Rights Clearinghouse. Empowering Consumers. Protecting Privacy. http://www. privacyrights.org.

[12] L. Coppolino, S. D'Antonio, A. Garofalo, and L. Romano. Applying data mining techniques to intrusion detection in wireless sensor networks. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on, pages 247–254, Oct 2013.

[13] Kaustav Das and Jeff Schneider. Detecting anomalous records in categorical datasets. In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, pages 220–229. ACM Press, 2007.

[14] T. Eswari and V. Vanitha. A novel rule based intrusion detection framework for wireless sensor networks. In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, pages 1019–1022, Feb 2013.

[15] International Organization for Standardization. ISO 3166-2:IT Standard. http://it.wikipedia. org/wiki/ISO_3166-2:IT.

[16] International Organization for Standardization. ISO 3166-2:IT Standard. http://loinc.org/.

[17] International Organization for Standardization. ISO iso 8601 Standard. http://en.wikipedia. org/wiki/ISO_8601.

[18] Hong Han, Xian-Liang Lu, and Li-Yong Ren. Using data mining to discover signatures in network-based intrusion detection. In Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on, volume 1, pages 13–17 vol.1, 2002.

[19] A. Husagic-Selman, R. Koker, and S. Selman. Intrusion detection using neural network committee machine. In Information, Communication and Automation Technologies (ICAT), 2013 XXIV International Symposium on, pages 1–6, Oct 2013.

[20] K. Ilgun, R.A. Kemmerer, and P.A. Porras. State transition analysis: a rule-based intrusion detection approach. Software Engineering, IEEE Transactions on, 21(3):181–199, Mar 1995.

[21] KNIME.com AG. Open for innovation KNIME. https://www.knime.org.

[22] C. Ko. System health and intrusion monitoring (shim): project summary. In DARPA Information Survivability Conference and Exposition, 2003. Proceedings, volume 2, pages 202–207 vol.2, April 2003.

[23] Calvin Ko. System health and intrusion monitoring: Technology description. In DISCEX (2), pages 27–29. IEEE Computer Society, 2003.

[24] A Menon, X. Jiang, J Kim, J Vaidya, and L Ohno-Machado. Detecting inappropriate access to electronic health records using collaborative filtering. Machine Learning for Science and Society, 2013.
[25] Peter G. Neumann and Phillip A. Porras. Experience with emerald to date. In Proceedings of the Workshop on Intrusion Detection and Network Monitoring, pages 73–80, Berkeley, CA, USA, 1999. USENIX Association.
[26] The University of Waikato. Waikato Environment for Knowledge Analysis - WEKA. http://www.cs. waikato.ac.nz/ml/weka/.
[27] U.S. Department of Homeland Security. What Is Critical Infrastructure? http://www.dhs.gov/ what-critical-infrastructure, Novembre 2013.
[28] Huaibin Wang and Boting Chen. Intrusion detection system based on multi-strategy pruning algorithm of the decision tree. In Grey Systems and Intelligent Services, 2013 IEEE International Conference on, pages 445–447, Nov 2013.
[29] Wen-Fang Yu and Na Wang. Research on credit card fraud detection model based on distance sum. In Artificial Intelligence, 2009. JCAI '09. International Joint Conference on, pages 353–356, April 2009.