# Decide Now or Decide Later? Quantifying the Tradeoff between Prospective and Retrospective Access Decisions

Wen Zhang[1], You Chen[2], Thaddeus R. Cybulski[4], Daniel Fabbri[1,2], Carl A. Gunter[3], Patrick Lawlor[4] , David Liebovitz[5], Bradley Malin[1,2]

[1]EECS Dept.
[2]Biomedical Informatics Dept.
Vanderbilt University
Nashville, TN, USA

[3]Dept. of Computer Science
University of Illinois
Urbana, IL, USA

[4]Dept. of PM&R
[5]Dept. of Medicine
Northwestern University
Chicago, IL, USA

{wen.zhang.1, b.malin, you.chen, daniel.fabbri}@vanderbilt.edu, cgunter@illinois.edu
{DavidL, cyb, patrick-lawlor}@northwestern.edu

## ABSTRACT

One of the greatest challenges an organization faces is determining when an employee is permitted to utilize a certain resource in a system. This "insider threat" can be addressed through two strategies: i) *prospective* methods, such as access control, that make a decision at the time of a request, and ii) *retrospective* methods, such as *post hoc* auditing, that make a decision in the light of the knowledge gathered afterwards. While it is recognized that each strategy has a distinct set of benefits and drawbacks, there has been little investigation into how to provide system administrators with practical guidance on when one or the other should be applied. To address this problem, we introduce a framework to compare these strategies on a common quantitative scale. In doing so, we translate these strategies into classification problems using a context-based feature space that assesses the likelihood that an access request is legitimate. We then introduce a technique called *bispective analysis* to compare the performance of the classification models under the situation of non-equivalent costs for false positive and negative instances, a significant extension on traditional cost analysis techniques, such as analysis of the receiver operator characteristic (ROC) curve. Using domain-specific cost estimates and access logs of several months from a large Electronic Medical Record (EMR) system, we demonstrate how bispective analysis can support meaningful decisions about the relative merits of prospective and retrospective decision making for specific types of hospital personnel.

*CCS'14,* November 3–7, 2014, Scottsdale, Arizona, USA.
Copyright 2014 ACM 978-1-4503-2957-6/14/11 ...$15.00.
http://dx.doi.org/10.1145/2660267.2660341 .

## Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access Control*; H.2.8 [**Database Management**]: Database Applications—*Data mining*

## General Terms

Security, Algorithms

## Keywords

access control, audit, context, data mining, decision support

## 1. INTRODUCTION

A fundamental tradeoff in authorization pits making a decision prospectively, before access is granted, against making a decision retrospectively, when an audit is carried out. Much of the work on access control has focused on the prospective decision making, but it has often been pointed out [15, 20] that retrospective decision making, in which users beg for forgiveness rather than permission, has some significant advantages. In many applications: (1) it is difficult to determine what access a user requires in advance, (2) denying access to a user with a legitimate need could result in significant inconvenience, expense, or loss, (3) most users are responsible and can be trusted to access resources for legitimate reasons, and (4) accountability (such as disciplinary action) is effective in deterring abuses. An iconic example of such a situation is access to patient records in Electronic Medical Record (EMR) systems, where (1) hospital workflows are complex and commonly involve emergencies and unexpected events, (2) lack of timely access could result in the loss of a patient's life, (3) most healthcare providers are highly trained and ethical professionals, and (4) there are strong penalties for abuse. These four criteria (and others, such as the ability in certain cases to roll back an illegitimate action) provide a good qualitative story for when retrospective decision-making based on audit may be better than prospective decision-making based on preventing access to a resource. We see the phenomena in many non-computer contexts already. For example, a red light tells a driver not to cross an intersection, but it does not prevent the driver from crossing it. On the other hand, there are instances where retrospective techniques are inadequate or too risky: the honor system may not be sufficient if the stakes for abuse are too high and the effectiveness of accountability is too low.

Given the recognition that retrospective techniques will have their place, we are led to ask: is there any systematic way to determine when retrospective techniques are better than prospective ones? Ideally this would be done quantitatively by measuring the tradeoff between the risks of addressing an abuse at audit time versus denying access to user when it is requested. If we accept the idea that the implementation of access control provides, in general, only an approximation of the desired access rules, then we may be able to quantify the rules with a Receiver Operating Curve (ROC) that compares false positives to true positives (a technique commonly used already for biometric authentication systems [18]). Better decision making then means better Area Under the ROC Curve (AUC) values. For example, if we are able to estimate that a prospective access control system gives proper access 95% of the time (true positives), but only if we accept that 10% of the time it will grant access where access should not have been granted (false positives), then we are on the path to quantify whether one type of prospective access is better than another. However, this does not offer a clear way to compare prospective techniques with retrospective ones. The latter, which can use information from both before and after a user has accessed a record, is expected to have better AUC values. The problem is that we do not have a cost model that allows us to judge tradeoffs between a pair of ROCs.

The aim of this paper is introduce a technique called *bispective analysis* that can be used to compare prospective and retrospective techniques for access control by a model that accounts for the different costs associated with false positives and negatives associated with each model. This is accomplished by weighting the ROC models for prospective and retrospective techniques by their costs and, subsequently, combining these in a way that enables direct comparison to see which is better in which circumstance. The primary contributions are:

- **A Novel Cost Analysis Technique** We devise a novel cost comparison method called bispective analysis that allows for an explicit comparison of classification models with different costs. Once provided with the knowledge of the variables (i.e., the costs of false positive and false negative for prospective model, the costs of false positive and false negative for retrospective, and the receiver operator characteristic (ROC) curves for both models), bispective analysis allows administrators to calculate which is the better option. Moreover, bispective analysis provides insight about the distribution of results under varying cost models, such that administrators can make decisions when their confidence in the variables is uncertain (e.g., only a range of costs are known or only partial costs are known).

- **Classification Models for Prospective and Retrospective Security** We develop a technique to represent and evaluate both prospective and retrospective models. To do so, we translate the context associated (e.g., other users who accessed a record, when the access was committed, and where the entity associated with the record was located) with each access into a vector space representation. We then subject such vectors to a classical machine learning model to build classifiers. In this way, prospective model and retrospective model are mapped to a common framework, such that comparable results can be generated. In addition, due to its simplicity and compactness in representation, this technique is scalable and adaptable to most information systems.

- **Empirical Analysis and Case Study** We illustrate how to apply bispective analysis to analyze tradeoffs for a large urban hospital system based on its EMR audit logs to provide assessments for various positions at the hospital. We deploy prospective and retrospective models implemented by the proposed technique in this system, and then obtain detection results (i.e, false positive rate, false negative rate) respectively. With bispective analysis and our detection results, we conduct illustrative case studies about the model selection with different assumptions on costs. In doing so, we assess how the model plays out for ten care provider positions in the system. The results show how cost weighting can yields different guidance in comparison to a standard ROC analysis.

The remainder of this paper is organized as follows. Section 2 provides a survey of cost-driven security models and comparison methods for classification methods. Section 3 describes foundational concepts, cost function, ROC curve and traditional cost analysis methods, including ROC convex hull methods and cost curves. Section 4 introduces bispective analysis. Section 5 presents the dataset preparation and experimental design. Section 6 introduces analysis on dataset by traditional methods. Section 7 presents experiment with bispective analysis on dataset and case studies showing the application of bispective analysis in real environment. Section 8 discusses potential extensions and variations of the proposed technique and some limitations of this work. Finally, Section 9 concludes the paper and suggests next steps for extending this work.

## 2. RELATED WORK

In this section, we review how existing cost-based security models differ from our work. We then review methodologies to compare classification models and the limitations associated with applying them to the prospective versus retrospective model analysis.

### 2.1 Cost-based Security Models

According to the National Institutes of Standards and Technologies [6], organizations should rate their information systems in terms of risk across three class: i) low, ii) medium, or iii) high. An organization should then adopt their security protections proportional to such risk. However, the selected security control may not be appropriate in that the rating for impact is highly subjective.

To reduce subjectivity in decision making, several risk-based strategies have been suggested for information security management. In particular, based on the recognition that business processes are often disrupted by static and rigid policies, many of these strategies are focused on access control. Here we review the approaches most related to our own. First, [5] proposed an adaptive access control model to balance the tradeoff between risk and utility in dynamic environments. They create a system that encourages information sharing among multiple organizations while keeping its users accountable for their actions and capping the expected damage an organization could suffer due to sensitive information disclosure. In relation to our own work, they introduce a method to compute the expected risk based on 1) the uncertainty and 2) the cost associated with an incorrect decision. Second, [13], introduced a policy-based access control model to infer a decision for an incoming access. This is achieved by training classifiers, using machine learning, on known decisions and subsequently inferring the new decision when there is no exact matching pattern. By doing so, each access decision is assigned a certain degree of risk. Third, [21] introduced the Benefit and Risk Access Control (BARAC) system, which identifies a set of correlated access requests as a closed system. Based on this system, this method uses a graph-based model to make a decision for each access, such that the cost of the entire system is minimized. All of these lines of research are significantly different from our own in that they focus on decisions between prospective access control models with constant misclassification costs, whereas we investigate a decision between prospective and retrospective models with varying costs.

## 2.2 Comparison of Classification Models

There are a number of performance measures that can be applied to assess the robustness of a classification model. For instance, one could assess the accuracy; i.e., the proportion of total instances that are correctly labeled by the model. However, accuracy is a biased assessment because it assumes that false positives and negatives occur at the same rate and are equally costly. As such, a more nuanced strategy for assessing classification models is to measure the ROC under a range of acceptance levels for false positive and false negative thresholds. In doing so, the AUC indicates the agility of a classifier, where the "best" classifier is the one that maximizes this value. The AUC has been invoked as a common approach for assessing various classification models for information security, such as intrusion detection systems (e.g., [12]), malware detection (e.g., [11]), and auditing techniques for EMRs (e.g., [1]). We recognize the relevance of machine learning (for which AUC is a popular evaluation measure), for information security has been questioned [19]. Yet, we stress that our goal is to assess how misclassification costs, rather than the machine learning algorithm itself, influence information security decisions. AUC also has serious deficencies in itself, 1)it is misleading when ROC curves cross and 2) it makes an unrealistic assumption on costs [8].

[16] proposed using a method to analyze the ROC convex hull to compose a dominant classification strategy over a set of classifiers and class frequencies (in the form of prior probabilities). This method begins by constructing a convex hull from all ROC curves (classifiers) to be compared, and then determines which point in the convex hull corresponds to the least overall cost, given the costs of each classifier and prior probabilities. A key advantage of this method is that it needs only the ratio of costs and ratio of class frequencies to compose the optimal classifier, such that it is robust to a changing environment.

Subsequently, [7] introduced an alternative to traditional ROC analysis, which is called a cost curve. In this model, the expected cost of a classifier is represented as a function of costs and class frequencies, such that the expected cost can be computed explicitly. A cost curve provides several benefits over the traditional ROC convex hull, including: 1) given specific cost estimates and prior probabilities, it is easy to "read-off" the expected cost, 2) it is immediately clear which, if any, classifier is the dominant strategy, and 3) it is straightforward to determine how much one classifier outperforms another. Building on this work, [8] introduced an approach to compares classifiers by computing their expected overall cost, in terms of a unified assumption on the probability density function of the costs of false positives (negatives).

However, in all of these techniques, it is assumed that the costs (or cost distributions) of false positive (false negative) for both classifiers are equivalent. Yet, this is clearly not the case in our situation, which implies that such strategies could incorrectly select a model. In fact, we verify this to be the case in our empirical analysis.

# 3. PRELIMINARIES

This section begins by reviewing basic concepts in classifier performance evaluation that are relevant to our strategy. Next, we introduce the definition of the cost of a classifier. This is followed by a review of the concept of an ROC curve, and several ROC-based comparison methods for classifiers. Finally, we review the notion of *context*, which is used in the implementation of our prospective and retrospective models.

## 3.1 Basic Concepts

The application of a classifier to a test instance results in either a correct or an incorrect decision. To assess the performance of a classifier, we consider the rates of these results over a set of cases. In doing so, the following simple measures are relevant: 1) True Positive Rate ($tpr$): the fraction of positive samples correctly classified; 2) False Negative Rate ($fnr = 1 - tpr$): the fraction of positive samples misclassified; 3) True Negative Rate ($tnr$): the fraction of negative samples correctly classified; and 4) False Positive Rate ($fpr = 1 - tnr$): the fraction of negative samples misclassified. Finally we report 5) *Accuracy*: the fraction of all samples correctly classified.

For orientation, it should be made clear that false positive and negatives have different implications (and thus different costs) in prospective and retrospective systems. In the prospective system, a false positive indicates the system approves an illegitimate access, while a false negative indicates the system denies access to a legitimate request. In the retrospective system, a false positive indicates that no investigation is performed for an illegitimate access, while a false negative means the system recommends an investigation for a legitimate access.

## 3.2 Cost Function

The *cost* of a classifier can be represented by Equation 1 [16]. Let $\pi_1$ and $\pi_0$ be the prior probabilities of positive and negative cases, respectively, such that $\pi_0 = 1 - \pi_1$. Let $p_{10}$ and $p_{01}$ be the $fnr$ and $fpr$, respectively. And, let $c_{10} \in (0, \infty)$ and $c_{01} \in (0, \infty)$ be the associated costs for the $fnr$ and $fpr$, respectively. In the remainder of this paper, we refer to $c_{10}$ and $c_{01}$ as the *false negative cost* and *false positive cost*, respectively.

$$cost = \pi_1 p_{10} c_{10} + \pi_0 p_{01} c_{01} \qquad (1)$$

### 3.3 ROC Curve

The result of a probabilistic classifier is dependent on its parameterization. For example, the naïve Bayes classifier incorporates a threshold for the probability with which it claims a class label (e.g., negative versus positive) corresponds to a certain instance. Traditionally, the result of a classifier is represented by a $(fpr,\ tpr)$ pair. The ROC curve can be obtained by plotting these pairs with respect to a range of parameterizations of the classifier. And, the AUC [2] is a commonly used measure for the evaluation of classification models. The larger the $AUC$ of a classifier, the better its performance.

Now, in this setting, a classifier $A$ is said to dominate another classifier $B$ if for any point $(fpr_A,\ tpr_A)$, there exists a point $(fpr_B,\ tpr_B)$, such that $tpr_B > tpr_A$ and $fpr_B < tpr_A$. For example, in Figure 5(a), it can be seen that the ROC of the retrospective model dominates the ROC of the prospective model.

Given any combination of $\pi_1$, $\pi_0$, $c_{10}$ and $c_{01}$, $MIN(cost_A) < MIN(cost_B)$ will be true if $A$ dominates $B$ [16], where $MIN(cost_X)$ is the minimal value of cost over the ROC curve of classifier $X$. This proposition is true because the ROC of $A$ forms the convex hull for both $A$ and $B$, and the point $(fpr,\ tpr)$ that minimizes cost, for any combination of $\pi_1$, $\pi_0$, $c_{10}$ and $c_{01}$, is only located on the convex hull [16]. As noted in Section 2.2, a premise for the convex hull method is that the cost of a false positive (negative) is equivalent for both classifier $A$ and $B$. However, as we will show in our empirical analysis, selecting security models by identifying dominance is inappropriate in situations for which this premise fails to hold.

### 3.4 Cost Curve

In this section, we review the cost curve introduced in [7]. As mentioned in the previous section, the cost curve retains all the merits of the ROC curve, but provides for several notable benefits. Though it is also hampered by the assumption of equivalent costs (as mentioned above), it serves as a foundation of our cost analysis.

Given estimates for $\pi_1$, $c_{10}$, $\pi_0$ and $c_{01}$, we can discover a point on the ROC curve to minimize *cost*. It has been proven that only $W = \frac{\pi_0 c_{01}}{\pi_1 c_{10}}$ is needed to determine the point $(1 - \bar{p}_{10}, \bar{p}_{01})$ of ROC that can minimize $cost$[16].

[7] introduced the concept of a normalized expected cost, which is defined in equation 2. $(\pi_1 c_{10} + \pi_0 c_{01})$ in Equation 2 is the maximized *cost* because it indicates both $p_{10}$ and $p_{01}$ are equal to 1. In other words, the classifier has misclassified all samples. Thus, computing *normcost* corresponds to normalizing *cost* into the (0,1) range. In this model, $(1 - \bar{p}_{10}, \bar{p}_{01})$ in the ROC minimizes *normcost* as well.

$$\begin{aligned} normcost &= \frac{\pi_1 p_{10} c_{10} + \pi_0 p_{01} c_{01}}{\pi_1 c_{10} + \pi_0 c_{01}} \\ &= p_{10} \cdot \frac{1}{W+1} + p_{01} \cdot \frac{W}{W+1} \\ &= p_{10} \cdot (1 - K) + p_{01} \cdot K \end{aligned} \tag{2}$$

From Equation 2, we can state $K = W/(W{+}1) = \pi_0 c_{01}/(\pi_1 c_{10} + \pi_0 c_{01})$, which means $K$ and $W$ constitute a one-to-one mapping. So, the values for $\bar{p}_{10}$ and $\bar{p}_{01}$ can be determined by $K$. Thus, the minimized *normcost*, denoted by $normcost^*(K)$, can be represented by Equation 3. [7] provides a detailed method for deriving the curve of $normcost^*$ (i.e., the cost curve). We directly employ this method when a computation of $normcost^*$ is required, but, due to space limitations, we refer the reader to [7] for the details.

$$normcost^*(K) = \bar{p}_{10} \cdot (1 - K) + \bar{p}_{01} \cdot K \tag{3}$$

$K$ can be interpreted as the *false positive cost ratio*. Informally, this corresponds to the proportion of cost resulting from false positives.

### 3.5 Context

In this paper, we refer to the access event that is under review as the *target*. This event can be associated with a wide range of semantics, which we call the *context* around the target access. The access itself is a request to a resource that is issued by a user, but there is a variety of contextual information that surrounds the target.

We assume that the target access takes place in the midst of a workflow, which we represent as a sequence of accesses, such that each is associated with the same underlying resource. We will represent a workflow as $\epsilon = \langle e_1,\ e_2,\ \ldots,\ e_i,\ \ldots,\ e_l \rangle$. For illustration, Figure 1 depicts a series of accesses to a specific patient's EMR from the point of admission to discharge from a hospital. Here, $e_3$ is the target access and the corresponding workflow is $\langle e_1,e_2,e_3,e_4,e_5,e_6 \rangle$. Context can be extracted from the target access itself (e.g., the time this access occurs). It can also be extracted from the corresponding workflow (e.g, users participated in the workflow). Note the availability of context in a workflow for the prospective model and the retrospective model are different. The retrospective model can take advantage of the entire workflow, while the prospective model can only take advantage of the parts of the workflow that occur before the target access.

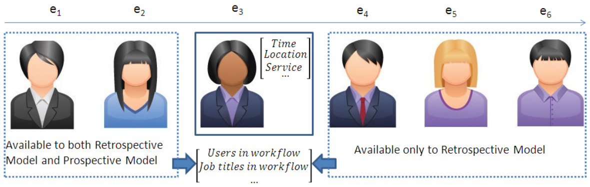

e1
e2
e3
e4
e5
e6
Time
Location
Service
...
Available to both Retrospective Model and Prospective Model
Users in workflow
Job titles in workflow
...
Available only to Retrospective Model

**Figure 1: An example of a workflow of accesses to a patient's medical record. Here, the target access $e_3$ is surrounded by a solid rectangle. The other accesses in the workflow are surrounded by a dashed rectangle. Parts contained by brackets represent context.**

## 4. FRAMEWORK

### 4.1 Framework Overview

To orient the reader, Figure 2 provides a high-level view of the proposed decision process for a specific user. As previous work shown [13], reliable access control policies (i.e., a prospective model) can be learned by a machine learning algorithm. We extend this notion for implementation of both the prospective model and the retrospective model. To do so, first, we extract workflows of targeted user from a database of transactions. Next, we construct vectors from the workflows to represent all accesses issued by the user. For the prospective model, the vectors are composed of contextual information that occurs at or before the point of a target access. For the retrospective model, the vectors are composed of context observed at any time (i.e., before, at or after the time of the target access). Next, the vectors are subject to a standard machine learning framework to build classifiers that are representative of prospective and retrospective models. Finally, a decision support system uses the ROC curves for the classifiers and their associated costs and returns an answer for which classifier (model) should be adopted to manage this specific user.

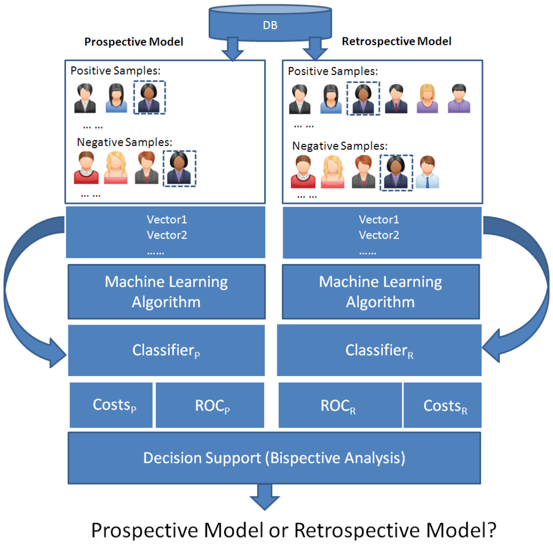


**Figure 2: An architectual view of the Bispective Analysis**

## 4.2 Decision Support

### 4.2.1 Bispective Analysis

As mentioned earlier, the prospective and retrospective security models are based on as machine learning algorithms. Traditional methods (e.g., ROC analysis) for comparing classifiers work under the belief that the costs for false positives (false negatives) are equivalent. However, this premise does not hold in the prospective versus retrospective security decision. Thus, we propose an analytic method called bispective analysis that extends cost curves to account for classifiers with differing misclassification costs. As will be illustrated, this method has a natural visual interpretation that can facilitate the decision making process.

To begin, equations 4 and 5 provide formulations for the overall cost of a prospective (P) and retrospective (R) model, respectively.

$$cost_P = \pi_1 p_{10}^{(P)} c_{10}^{(P)} + \pi_0 p_{01}^{(P)} c_{01}^{(P)} \tag{4}$$

$$cost_R = \pi_1 p_{10}^{(R)} c_{10}^{(R)} + \pi_0 p_{01}^{(R)} c_{01}^{(R)} \tag{5}$$

These functions allow us to derive a comparison function to compare the costs caused by the two models, denoted by equation 6.

$$comp(P,R) = ln(\frac{cost_P^*}{cost_R^*}) \tag{6}$$

Here, $cost_P^*$ and $cost_R^*$ correspond to the minimized overall costs given: i) the false positive (negative) costs estimates and ii) the prior distributions of positives and negatives. iii) the ROC curves. When $comp(P,R) > 0$, the prospective model incurs greater cost than the retrospective model (denoted by R $\succ$ P). When $comp(P,R) < 0$, the retrospective model incurs greater cost than the prospective model (denoted by R $\prec$ P). And, when $comp(P,R) = 0$, the prospective and retrospective models have equivalent costs (denoted by R $\simeq$ P).

The comparison function contains too many variables to be visualized in an interpretable manner. Thus, we reduce the number of variables via a mathematical deduction in Equation 7. Note we use the cost curve $normcost^*(K)$ in Equation 7. It can be seen that $comp(P,R)$ is a function of $K_P = \pi_0 c_{01}^{(P)} / (\pi_1 c_{10}^{(P)} + \pi_0 c_{01}^{(P)})$ , $K_R = \pi_0 c_{01}^{(R)} / (\pi_1 c_{10}^{(R)} + \pi_0 c_{01}^{(R)})$ and $ratio = c_{01}^{(P)} / c_{01}^{(R)}$. When $ratio$ is a constant $z$, the comparison function can be represented as $Magnitude($ $K_P$,$K_R)$, as shown in Equation 8. Given this representation, we can then compose a contour for $Magnitude(K_P, K_R)$ to investigate the tradeoffs under various cost conditions.

$$\begin{aligned} comp(P,R) &= ln(\frac{\pi_1 \bar{p}_{10}^{(P)} c_{10}^{(P)} + \pi_0 \bar{p}_{01}^{(P)} c_{01}^{(P)}}{\pi_1 \bar{p}_{10}^{(R)} c_{10}^{(R)} + \pi_0 \bar{p}_{01}^{(R)} c_{01}^{(R)}}) \\ &= ln(\frac{\pi_1 c_{10}^{(P)} + \pi_0 c_{01}^{(P)}}{\pi_1 c_{10}^{(R)} + \pi_0 c_{01}^{(R)}} \cdot \frac{\frac{\pi_1 \bar{p}_{10}^{(P)} c_{10}^{(P)} + \pi_0 \bar{p}_{01}^{(P)} c_{01}^{(P)}}{\pi_1 c_{10}^{(P)} + \pi_0 c_{01}^{(P)}}}{\frac{\pi_1 \bar{p}_{10}^{(R)} c_{10}^{(R)} + \pi_0 \bar{p}_{01}^{(R)} c_{01}^{(R)}}{\pi_1 c_{10}^{(R)} + \pi_0 c_{01}^{(R)}}}) \\ &= ln(\frac{c_{01}^{(P)}}{c_{01}^{(R)}} \cdot \frac{K_R}{K_P} \cdot \frac{normcost_P^*(K_P)}{normcost_R^*(K_R)}) \end{aligned} \tag{7}$$

$$\begin{aligned} Magnitude(K_P, K_R) &= comp(P,R)|_{ratio=z} \\ &= ln(z \cdot \frac{K_R}{K_P} \cdot \frac{normcost_P^*(K_P)}{normcost_R^*(K_R)}) \end{aligned} \tag{8}$$

Figure 3(a) depicts an example of such a contour for one user associated with the job title of *NMH Physician CPOE* (Computerized Provider Order Entry) in the EMR dataset of our case study. Each line in the contour plot, which we call a *contour line*, consists of the points ($K_P$, $K_R$) for which $Magnitude(K_P, K_R)$ has a constant value. This value is represented by the number on the contour line.

To further simplify the decision making process, we can compose a contour using Equation 9, where $sgn(\cdot)$ is the sign function. The value of *Threshold()* must be drawn from $\{-1, 0, 1\}$, which corresponds to $R \prec P$, $R \simeq P$ and $R \succ P$, respectively. Figure 3(b) provides an example of the contour after applying this threshold, where the red region corresponds to $R \succ P$, the blue region corresponds to $R \prec P$ and the boundary between them corresponds to $R \simeq P$. To provide guidance, the former contour should be utilized when the magnitude of difference between the prospective and respective models is of interest to an administrator (e.g., the trends of comparison results when $K_P$ and $K_R$ changes), while the latter should be chosen when the administrator is interested only in which model is dominant.

$$Threshold(K_P, K_R) = sgn(Magnitude(K_P, K_R)) \tag{9}$$

#### 4.2.2 Probability Computation with Comparison Function

Intuitively, in contour plot, the proportion of the area determined by $Threshold() = 1$ reflects the probability that the retrospective model will be the dominant strategy. For illustration, in Figure 3(b), the region shaded in red indicates the probability that retrospective is the dominant solution for the *NMH Physician CPOE* is very high.

This type of contour can enable an administrator to ascertain which model has a higher probability of effectiveness. To understand how, let us assume that $f(K_P, K_R)$ corresponds to the joint density function of $K_P$ and $K_R$. Now, $K_P$ and $K_R$ can be considered independent because they are derived from two distinct classification models. As a consequence, the probability that the retrospective model dominates the prospective model can be represented by Equation 10, where $f_P()$ and $f_R()$ indicate the density functions of $K_P$ and $K_R$, respectively.

$$\begin{aligned} Pr(R \succ P) &= \int_{Threshold(K_P,K_R)=1} f(K_P, K_R) dK_P dK_R \\ &= \int_{Threshold(K_P,K_R)=1} f_P(K_P) f_R(K_R) dK_P dK_R \end{aligned} \tag{10}$$

A common and reasonable assumption for $f_P()$ and $f_R()$ is the density function of the uniform distribution with range (0,1) [7, 14]. This is useful because, in combination with Equation 10, it follows that $Pr(R \succ P)$ corresponds to the proportion of the contour where $Threshold(K_P, K_R) = 1$. More formally, this is derived as follows

$$\begin{aligned} Pr(R \succ P) &= \int_{Threshold(K_P,K_R)=1} f_P(K_P) f_R(K_R) dK_P dK_R \\ &= \int_{Threshold(K_P,K_R)=1} 1 \cdot 1 dK_P dK_R \\ &= \int_{Threshold(K_P,K_R)=1} dK_P dK_R. \end{aligned} \tag{11}$$

### 4.3 Context-based Classification

The context-based classification consists of three steps: i) construct vectors from the workflows; ii) train a classifier on a subset of the vectors; and iii) test the classifier on the remainder of the vectors. Since this paper does not focus on a specific machine learning algorithm, here we focus on the process by which we construct vectors used for prospective and retrospective models.

#### 4.3.1 Prospective Model

We use $C = \{C_1, C_2, \ldots, C_h\}$ to denote the set of context that is associated with a target access. $C_r$ is composed of elements from $dom(C_r)$, which is the *domain* of elements associated with this type of context. For example, let $U \in C$ denote all users that attend the workflow of target access. As such, we have $dom(U) = \{u_1, u_2, \ldots, u_d\}$, such that $u_i$ is a certain user in the system.

In a prospective model, the system needs to make a decision once the target access $e_i$ has been issued. At the moment $e_i$ is issued, we only know the accesses transpiring beforehand, which corresponds to $\epsilon_1 = \langle e_1, e_2, \ldots, e_{i-1} \rangle$. For $e_i$, we can use vectors as representations of all $h$ types of context. Equation 12 denotes $V(U)$, the vector corresponding to context $U$.

$$V(U) = (v_{u_1}, v_{u_2}, \ldots, v_{u_d}) \tag{12}$$

In this model, $v_{u_x}$ is set to 1 if $u_x$ is observed when at least one $e_j \in \epsilon_1$ transpires, otherwise it is set to 0.

For example, imagine we want to construct a vector corresponding to $U$ (i.e., $V(U)$), for the target access $e_3$ in Figure 1. Let $dom(U) = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\}$ in the system and $\langle u_2, u_4, u_5, u_1, u_3, u_8 \rangle$ be the user sequence corresponding to the workflow in Figure 1. $\epsilon_1 = \langle e_1, e_2 \rangle$ is the access sequence occurring before $e_3$, where $e_1$ and $e_2$ are executed by $u_2$ and $u_4$ respectively. Thus, the vector corresponding to $U$ for target user is $(0, 1, 0, 1, 0, 0, 0, 0)$.

We use $\oplus$ to denote the union of two vectors[1]. As such, the vector for all $h$ context can be represented as $CV = V(C_1) \oplus V(C_2) \oplus \ldots \oplus V(C_h)$.

#### 4.3.2 Retrospective Model

A retrospective model is employed to review the target access using accesses occurring in the entire workflow. These accesses correspond to $\epsilon_0 = \langle e_1, e_2, \ldots, e_{i-1}, e_{i+1}, \ldots, e_l \rangle$. In this case, during construction of $V(U)$, $v_{u_x}$ is assigned 1, if user $u_x$ exists when at least one $e_j \in \epsilon_0$ transpires (i.e., $e_j$ is executed by $u_x$). In Figure 1, the user context vector of the retrospective model is $(1, 1, 1, 1, 0, 0, 0, 1)$. It is not necessary for the vector $V(C_r)$ in the prospective model and retrospective model to be different. For example, $V(C_r)$ will be identical for two models when $C_r$ denotes the time the target access was issued.

## 5. EXPERIMENTAL DESIGN

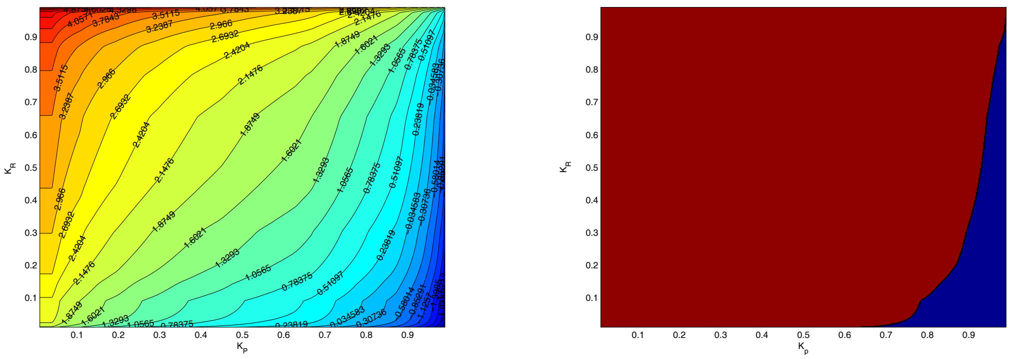
This section provides an overview of the experiments designed for this study. It begins with a description of the real electronic medical record (EMR) data. This is followed by an explanation of how context was modeled to train the prospective and the retrospective security models. We then introduce the machine learning algorithm used for training the models and the specific measures used for assessing their performance.

### 5.1 Electronic Medical Record

The dataset was extracted from three consecutive months of access logs from the Cerner Corporation's PowerChart EMR system in use at Northwestern Memorial Hospital, which is an 854 bed primary teaching affiliate of Northwestern University. All clinicians retrieve clinical information and enter inpatient notes and orders using the system. Each entry of the log contains information about a distinct access made to the EMR is associated with seven pieces of information: i) encounter-id, ii) user-id, iii) patient-id, iv) time, v) user job title, vi) service , and vii) location where the associated patient is located.

Let us take a moment to provide more detail on what this information corresponds to. Each (*patient-id*, *encounter-id*) pair defines a unique workflow for patient treatment. This

[1] For example, vector $C = \langle a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \rangle$ is the union of vector $A = \langle a_1, a_2, \ldots, a_m \rangle$ and vector $B = \langle b_1, b_2, \ldots, b_n \rangle$ (i.e., $C = A \oplus B$)



(a) Contour Plot for $Magnitude(K_P, K_R)$ (b) Contour Plot for $Threshold(K_P, K_R)$)

**Figure 3: Contour plots for the *NMH* Physician CPOE role in the NMH dataset. The red and blue regions correspond to when the retrospective and prospective models dominate, respectively.**

encounter begins when the patient is admitted to the hospital and ends two weeks after discharge (to ensure that accesses associated with medical billing are captured). Table 1 summarizes each context we use to represent an access and the size of its domain. Of the remaining information, there are five types of context: i) the time a target access was issued (Time)[2], ii) the hospital service the patient was on at the time of the target access (e.g., General Medicine vs. Obstetrics), iii) location in the medical center where the patient resided when the target access was issued, iv) the users who commit accesses in the workflow of target access and v) the job titles associated with these users.

**Table 1: The context used in experiment**

| | Users | Time | Job Titles | Services | Locations |
|---|---|---|---|---|---|
| \|Dom\| | 8095 | 4 | 140 | 43 | 58 |

## 5.2 Dataset Preparation

Without loss of generality, assume target user $t$ participates in $N$ patient workflows. The corresponding context vectors are $CV_1^+, CV_2^+, \ldots, CV_N^+$, which are composed using the approach described in Section 4.3. These vectors are associated with a *positive* label class. We use the following process to generate a corresponding set of $N$ *negative* labeled instances. We randomly select a workflow in which user $t$ failed to issue an access. From this workflow, we randomly select an access and build a corresponding context vector. Doing so $N$ times yields a set of vectors $CV_1^-, CV_2^-, \ldots, CV_N^-$, which are associated with the negative class. Note that we create different $CV_i^+$ and $CV_i^-$ for prospective model and retrospective model respectively.

To conduct our evaluation, we construct 10 datasets, each of which corresponds to a different job title. Let us use *Patient Care Staff Nurse* as an example. We randomly pick 10 users whose job titles are *Patient Care Staff Nurse*. For each user, we construct $N$ positive samples and $N$ negative samples using the process described above. We select 80% of the vectors from the positive and negative samples, respectively, for the training set, and use the remaining 20% as the test set. The samples generated for all 10 users are then combined to form a single dataset for this job title and the overall performance across the 10 users is measured to evalute the entire dataset. To ensure the results are representative, we select job titles from 10 different hospital departments. The job titles and summary statistics are shown in Table 2.

We train a classifier for each user using a support vector machine (SVM) using an RBF kernel [10]. We utilize a grid search technique [10] to find values for parameters to enable a robust SVM. For each user in the job title, we use the classifier trained on the training set of this user to assess the corresponding test set.

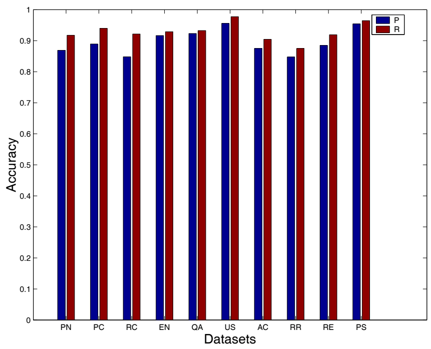


**Figure 4: Accuracy of the prospective and retrospective security models**

# 6. TRADITIONAL METHODS TO COMPARE MODELS

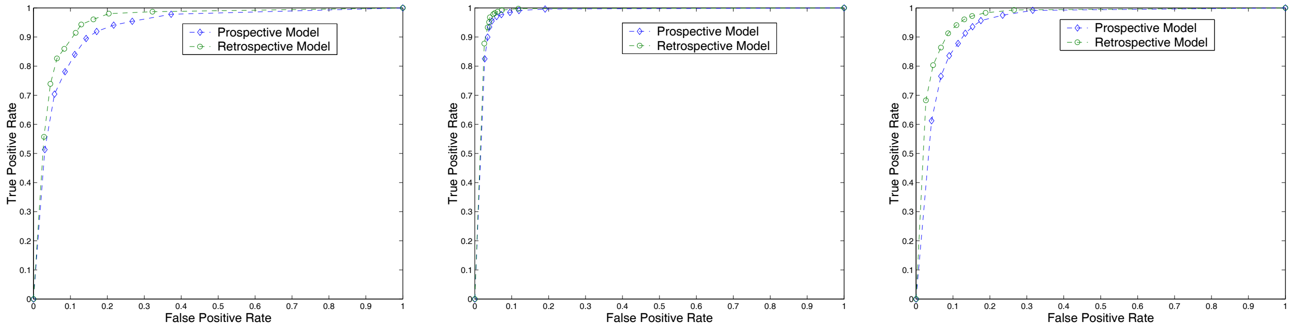
In this section, we compare prospective and retrospective security models using traditional evaluation strategies to set a baseline. We observe what kind of decision would be made by these traditional strategies, and figure out they may make unwise decision sometimes.

First, Figure 4 presents the accuracy of both the prospective model and the retrospective model on 10 datasets. It can be seen that the retrospective model has a higher accuracy than the prospective model for each job title. This evidence supports the hypothesis that contextual information

[2] For this work, $dom(Time)$ consists of four values: a) Morning (6am - 12pm), b) Afternoon (12pm - 6pm), c) Evening (6pm - 12am), and d) Night (12am - 6am)

**Table 2: Datasets per job titles and the $AUC$ for their corresponding prospective and retrospective models.**

| Abbrev. | Job Title | Instances Per Class | $AUC_P$ | $AUC_R$ |
|---|---|---|---|---|
| US | Unit Secretary | 1839 | 0.984 | 0.994 |
| QA | Utilization Review/Quality Assurance 1 | 1069 | 0.959 | 0.972 |
| PS | Patient Care Assistive Staff | 777 | 0.979 | 0.983 |
| RE | Rehabilitation - Physical Therapist | 712 | 0.944 | 0.964 |
| RC | Resident/Fellow CPOE | 504 | 0.925 | 0.967 |
| AC | Anesthesia CPOE | 456 | 0.932 | 0.953 |
| PC | NMH Physician CPOE | 448 | 0.953 | 0.979 |
| PN | Patient Care Staff Nurse | 382 | 0.939 | 0.959 |
| EN | Emergency Department Patient Care Staff Nurse | 366 | 0.961 | 0.976 |
| RR | Radiology Resident/Fellow | 364 | 0.919 | 0.944 |



(a) ROC of $AC$ (b) ROC of $PS$ (c) ROC of $RE$

**Figure 5: ROC curves for the prospective and retrospective models of three job titles.**

obtained after a target access can lead to better classification performance. Simply put, an retrospective model can yield a more correct assessment of an access request. Moreover, from Table 2 it can be observed that $AUC_R$ is larger than $AUC_P$ for every job title, which further indicates that retrospective security models are better than prospective security models under a traditional assumption of costs.

Next, we inspected the ROC curves of the prospective and retrospective models. The curves for three of the job titles are depicted in Figure 5. From the ROC curves, we find that the retrospective model dominates the prospective model for the three datasets. This indicates that, if the assumption of equal costs for false positive (negative) holds true, then the retrospective model will always be chosen regardless of the false positive (negative) cost estimation and prior positive (negative) probability. The cost curve is considered a dual representation of the ROC curve. This means using cost curve would reach the same conclusion (i.e., retrospective model wins) as the ROC curve for the job titles studied. As such, we do not present the cost curve in this section.

The assumption of equal costs for security-related classifiers is made in almost all previous research. And, if a security professional worked under this belief, then retrospective protections would almost be utilized over prospective models. However, as has been alluded to, this assumption certainly does not hold and, as the following results will illustrate, can unnecessarily justify costly behavior.

# 7. HOW THE BISPECTIVE ANALYSIS INFLUENCES SECURITY DECISIONS

This section shows how our proposed technique affects the prospective versus retrospective decision model. First, we draw a series of contour plots for $Magnitude(K_P, K_R)$ or $Threshold(K_P, K_R)$ under a different $ratio = c_{01}^{(P)}/c_{01}^{(R)}$ for job title *Radiology Resident/Fellow*. We demonstrate how prospective and retrospective models can be compared from various pespective. Then, we present several case studies to show the application of our cost analysis technique in real environments, which demonstrates our technique can make a more reasonable decision than traditional methods.

## 7.1 Make Decision with Bispective Analysis

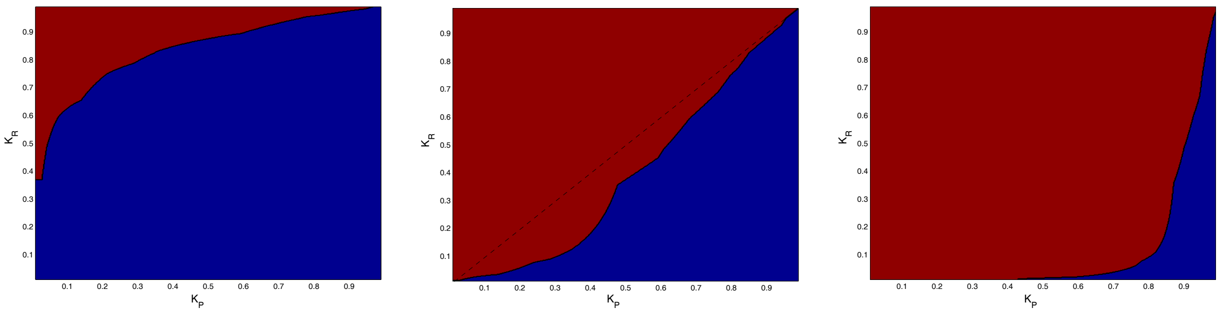
Figure 6 shows the contour plots of $Threshold(K_P, K_R)$ for the *Radiology Resident/Fellow* job title. With full knowledge about costs and the prior distribution of positive and negative instances, we can determine which security is best by pinpointing the corresponding coordinate in the plot. We will present case studies later to show this process in detail. With uncertainty in costs and prior distributions, bispective analysis can still be conducted through the contour plots from various perspectives, as we now illustrate.

### 7.1.1 Probability Analysis

According to section 4.2.2, the area of the region in the contour plot determined by $Threshold(K_P, K_R) = 1$ equals the probability that $R \succ P$. Now, assume that we already know $ratio = 0.3$. Then, if we look at the contour plot corresponding to $ratio = 0.3$ in Figure 6(a), it is clear that $P(R \succ P) < 0.5$. This means that an administrator should choose a prospective model to manage the accesses from *Radiology Resident/Fellow* when only $ratio = 0.3$ is known.

### 7.1.2 Range Narrowing Analysis

In certain instances, with limited knowledge of costs and prior distributions, the search space can be narrowed into a small area. When this is possible, it can provide a clear solution to which model should be selected, even if such a



(a) $raito = 0.3$ (b) $ratio = 1.0$ (c) $ratio = 3.0$

**Figure 6: Contour plots for $Threshold(K_P, K_R)$ with different $ratio$ for the *Radiology Resident/Fellow*. The red and blue regions correspond to when the retrospective and prospective models dominate, respectively.**

decision was not possible in general. For instance, in an hospital system, the following assumptions about costs for misclassification in prospective and retrospective systems:

$$c_{01}^{(P)} \approx c_{01}^{(R)} \tag{13}$$

$$c_{10}^{(P)} > c_{10}^{(R)} \tag{14}$$

The first assumption (Equation 13) states that the cost of the prospective system allowing a malicious access and the cost of the retrospective system failing to identify a malicious access are approximately equal. The second assumption (Inequation 14) states that the cost of a prospective system blocking an access from *Radiology Resident/Fellow* would be greater than that of a retrospective system incorrectly identifying a normal and historical access from this job title as malicious. We will discuss how these assumptions are justified in our case studies. When such an assumption holds, we should look at Figure 6(b), which is a contour plot of $Threshold(K_P, K_R)$ given $ratio = c_{01}^{(P)}/c_{01}^{(R)} = 1.0$. Additionally, based on these assumptions, it follows that $K_P - K_R < 0$ because the numerator of $K_P$ and $K_R$ are equal according to $c_{01}^{(P)} \approx c_{01}^{(R)}$, and denominator of $K_P$ would be larger than that of $K_R$ according to $c_{01}^{(P)} \approx c_{01}^{(R)}$ and $c_{10}^{(P)} > c_{10}^{(R)}$. In Figure 6(b), it can be seen that the $K_P - K_R < 0$ is always located at the left of the diagonal (i.e., the black dashed line in the figure), a region where the retrospective security model is always dominant.

Note that when $c_{01}^{(P)} = c_{01}^{(R)}$ and $c_{10}^{(P)} = c_{10}^{(R)}$ (i.e., the premise that false positive (negative) costs are equal across two models holds), we have $K_P - K_R = 0$, which corresponds to the dashed line in Figure 6(b). That means our bispective analysis can still work under the permise as is believed in traditional ROC analysis.

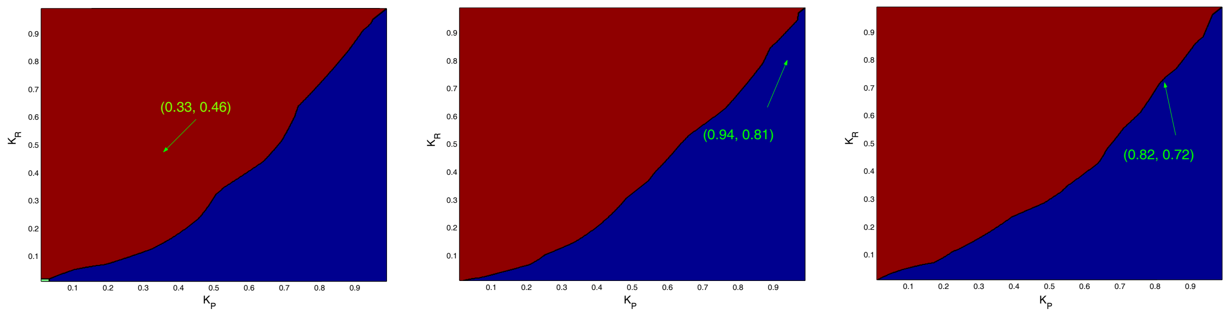
## 7.2 Case Studies

In this section, we show three examples of bispective analysis in the domain of healthcare. We consider three job titles, Patient Care Assistive Staff and Anesthesia CPOE, and Rehabilitation - Physical Therapist, estimating $c_{01}^{(P)}$, $c_{01}^{(R)}$, $c_{10}^{(P)}$, and $c_{10}^{(R)}$ for each job title, and then apply bispective analysis to determine if a prospective or a retrospective models should be applied on this job title. We show that, for some jobs, choosing a prospective model will minimize cost, disagreeing with techniques that do not take cost into account. The estimations described are by no means exhaustive; rather they exist to demonstrate the utility of a cost-based decision support.

### 7.2.1 Cost Estimation

$c_{01}^{(P)}$ represents the costs of allowing an inappropriate access under a prospective model, while $c_{01}^{(R)}$ represents the costs of deciding not to review an illegitimate access under a retrospective model. These costs are generally the result of fines under HIPAA, HITECH, and other heathcare security statues. As the fines associated with inappropriate access are likely relatively independent of the security model that they were performed under, we assume equality of $c_{01}^{(P)}$ and $c_{01}^{(R)}$. We also assume that fines due to inappropriate accesses are equivalent regardless of who makes them. For the sake of example, fines for inappropriate access over eight separate incidents in California hospitals ranged from \$5,000 to \$225,000, averaging \$18,546 per inappropriate access [4, 17]. Costs associated with inappropriate access will vary due to jurisdiction and individual details, we use this average as both $c_{01}^{(P)}$ and $c_{01}^{(R)}$ for the three job titles.

$c_{10}^{(P)}$ represents denying a legitimate access under a prospective model. This is likely the most difficult cost to estimate, as it alters behavior in a way that is not currently present in medical settings. For Patient Care Assistive Staff, which generally would be assisting another employee that has chart access permission, we can estimate $c_{10}^{(P)}$ as an hour of personnel time with no other costs. The national average wage for medical assistive staff is \$11.73 [3]. For Anesthesia CPOE, in the best case, withholding physician access to a patient chart would cause the physician to wait, incurring a cost of only an hour of personnel time. The national average hourly compensation for anesthesiologists is \$183 [9]. However, withholding access during a high-risk, high-urgency situation could result in a number of adverse outcomes, such as misdiagnosis or drug interactions, reducing quality of care and introducing the prospect of legal action. There is very little data on such a scenario. We estimate $c_{10}^{(P)}$ for Anesthesia CPOE to be \$500, although it could range from our conservative estimate of \$183 to something orders of magnitude higher depending on physician behavior. Physical therapists generally work in low-urgency situations, so ad-



(a) Contour for AC when $ratio = 1$ (b) Contour for PS when $ratio = 1$ (c) Contour for RE when $ratio = 1$

**Figure 7: Case Study Contour Plots**

verse outcomes are significantly less likely. We estimate $c_{10}^{(P)}$ for them as $39.51, the national average wage [3].

$c_{10}^{(R)}$ represents the costs associated with auditing a legitimate access. We assume that this decision only incurs costs related to personnel time, specifically an hour of auditor time at $32.10 [3], again the national average for compliance officers, and an hour of time from the individual being audited. Thus $c_{10}^{(R)}$ for Patient Care Assistive Staff is approximately $43.83, while $c_{10}^{(R)}$ for Anesthesia CPOE is approximately $215, and $c_{10}^{(R)}$ for Rehabilitation - Physical Therapist is $71.61.

**Table 3: Cost Estimation**

| | $c_{01}^{(P)}$ | $c_{01}^{(R)}$ | $c_{10}^{(P)}$ | $c_{10}^{(R)}$ | $K_P$ | $K_R$ |
|---|---|---|---|---|---|---|
| PS | $18,546 | $18,546 | $11.73 | $43.84 | 0.94 | 0.81 |
| AC | $18,546 | $18,546 | $183 | $215.10 | 0.33 | 0.46 |
| RE | $18,546 | $18,546 | $39.51 | $71.61 | 0.82 | 0.72 |

### 7.2.2 *Bispective Analysis on Three Job titles*

The resulting values of $K_P$ and $K_R$ for Patient Care Assistive Staff (PS), Anesthesia CPOE (AC) and Rehabilitation-Physical Therapist (RE) are in Table 3, assuming 1% of accesses are inappropriate. Using the contour plots in Figure 7, we can make the following observations. For AC, a retrospective model minimizes cost. For PS, a prospective model minimizes cost. For RE, bispective analysis shows the prospective model minimizes cost (or at least no preference between the two). Remember if we use traditional methods, retrospective models would be chosen for all three job titles.

# 8. DISCUSSION

## 8.1 Extensions

In Section 4.2.1, we derive functions for contour plot drawing by fixing *ratio*. Likewise, we can also derive two other two-variables functions by fixing $K_P$ or $K_R$. This assures that we can still produce contour plots for decision making when we only have the estimation of $K_P$ or $K_R$ rather than *ratio*. In addition, we note that the *comp*() function can also be a function of $ratio1 = c_{10}^{(P)}/c_{10}^{(R)}$, $K_P$ and $K_R$. That means we can obtain a contour plot when only $ratio1$ is known. In summary, the visualized analysis for decision can be performed when value of only one of *ratio*, $ratio1$, $K_P$ and $K_R$ is known.

In addition, note that the final decision is made on a role-basis in our experiment. That means once one of the two security models is selected by applying our technique and deployed in the system, all access requests from users in this role would be evaluated by this model. In practice, there may exist a big variance among users in the same role. Specifically, there can be different ROC curves for different users in the same role. In this situation, it is inappropriate to apply an unified security model for all users of the role. Instead, administrator would need to conduct personalized model selection by applying our framework to each user separately.

## 8.2 Limitations

Our decision support method relies heavily on the contour plot of comparison function of two models. That means we may need $C_n^2{=}n(n-1)/2$ contour plots when there are options of $n$ models. When $n$ is a large number, we would need to study too many contour plots to make a decision, which would offset the visual convenience of contour plot.

Another limitation is that the cost function used in this paper assumes correct classification does not incur cost, which however is not the case in reality. For example, let us consider retrospective model in hospital system. Assume a user issued a malicious access to a patient's record in the system, and was identified later by retrospective system. Even though the user would be penalized, it is possible the patient's information has already been leaked to the public, which would lead to costly consequence.

# 9. CONCLUSIONS

This paper proposed a novel framework that enables organizations to perform comparison between prospective and retrospective models on a quantitative scale. Developing such a framework addresses two challenges. First, existing prospective and retrospective models are semantically different such that their results are not directly comparable. Second, the assumption that costs of false positive (and false negative) are equivalent across the classifiers needs to hold for existing technique to conduct cost analysis of multiple classifiers. To address the first challenge, we converted the two security models (i.e., prospective and retrospective) into a unified classification models by training the same classifiers on the data represented by the same set of features (contexts). To address the second challenge, we devise a visualized analysis method, named bispective analysis, that leverage contour plot of a comparison function to provide a direct decision support for administrator. We then experimented on a real hospital information system with this framework to show that it can provide good decision support quality. Somewhat surprisingly, we also found it can provide decision support even when knowledge about costs are insufficient.

This work opens up a wide array of opportunities for feature security research. First, we assumed that prospective analysis would be done after a workflow ends. Yet, in practice, it could start at any time after the target access happens. It is worth extending our work to implement such a prospective system for comparison. Second, cost analysis method can be extended to handle the situation that cost for correct classification is not equal to zero.

## 10. ACKNOWLEDGEMENTS

This research was supported by grants CCF-0424422, CNS-0964063, CNS-0964392 and CNS-1330491 from the National Science Foundation (NSF), R01-LM010207 from the National Institutes of Health (NIH), and HHS-90TR0003/01 from the Office of the National Coordinator for Health Information Technology at the Department of Health and Human Services (HHS). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS, NIH, or NSF. The authors also thank Nathan Sisterson for supplying the dataset used in this study.

## 11. REFERENCES

[1] A. A. Boxwala, J. Kim, J. M. Grillo, and L. 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.

[2] A. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. *Pattern Recognition*, 30:1145–1159, 1997.

[3] Bureau of Labor Statistics and U.S. Department of Labor. Occupational outlook handbook, 2014-15 edition, 2014.

[4] California Department of Public Health. California Department of Public Health Issues Privacy Breach Fines to 7 California Health Facilities, 2010.

[5] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 222–230, 2007.

[6] K. Dempsey, G. Witte, and D. Rike. Security and privacy controls for federal information system and organizations. Technical Report Special Publication 800-53, Revision 4, Washington, DC, 2014.

[7] C. Drummond and R. Holte. Explicitly representing expected cost: an alternative to roc representation. In *Proceedings of the* $6^{th}$ *international conference on Knowledge Discovery and Data Mining*, pages 198–207, 2000.

[8] D. Hand. Measuring classifier performance: a coherent alternative to the area under the roc curve. *Machine Learning*, 77:103–123, 2009.

[9] B. Herman. 72 Statistics on Hourly Physician Compensation, 2013.

[10] C. W. Hsu, C. C. Chang, and C. J. Lin. A practical guide to support vector classification. Technical report, Dept. of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, 2003.

[11] J. Z. Kolter and M. A. Maloof. Learning to detect malicious executables in the wild. In *Proceedings of the* $10^{th}$ *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 470–478, 2004.

[12] R. Lippmann, D. Fried, I. Grad, et al. Evaluating intrusion detection systems: the 1998 darpa off-line intrusion detection evaluation. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, pages 12–26, 2000.

[13] I. Molloy, P. Cheng, J. Dicken, A. Russo, and C. Morisset. Risk-based access control decisions under uncertainty. In *Proceedings of the* $2^{nd}$ *ACM conference on Data and Application Security and Privacy*, pages 157–168, 2012.

[14] J. H. Orallo, P. Flach, and C. Ferri. A unified view of performance metrics: Translating threshold choices into expected classification loss. *Journal of Machine Learning Research*, 13:2813–2869, 2012.

[15] D. Povey. Optimistic security: a new access control paradigm. In *Proceedings of the Workshop on New Security Paradigms*, pages 40–45, 1999.

[16] F. Provost and T. Fawcett. Analysis and visualization of classifier performance: Comparison under imprecise class and cost distributions. In *Proceedings of the* $3^{rd}$ *international conference on Knowledge Discovery and Data Mining*, pages 43–48, 1997.

[17] K. Robertson. Kaiser fined for employees checking medical records of octuplets - Sacramento Business Journal, 2009.

[18] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3):450–455, 2005.

[19] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 305–316, 2010.

[20] D. Weitzner. Information accountability. *Communications of the ACM*, 37(6):82–87, 2008.

[21] L. Zhang, A. Brodsky, and S. Jajodia. Toward information sharing: Benefit and risk access control. In *Proceedings of the* $7^{th}$ *IEEE International Workshop on Policies for Distributed Systems and Networks*, pages 45–53, 2006.