Finding needle in the case-stack: Effective remote monitoring of courts

Amm Rahman, Hassan Nawaz, Omer Naeem, Fareed Zaffar, Farooq Naseer, Adeel Zaffar
LUMS, Lahore University of Management Sciences
Lahore, Pakistan
{amm.rahman,hassan.nawaz,omer.naeem,fareed.zaffar,farooq.naseer,adeel.zaffar}@lums.edu.pk

Abstract

Delay in the judicial processes and pendency of existing cases is an old problem that has defied easy solutions in Pakistan. Most cases are trapped in the system due to a huge backlog of cases, excessive litigation in urban areas, corruption by the court staff and lack of proper monitoring of the functioning of courts. Efficient supervision and monitoring of courts can help in resolving some of the key problems in the system. We present preliminary results from a novel case record-keeping, management and monitoring solution that is able to meet several key performance goals of the National Judicial Policy. The overall aim of the work is to facilitate the work of the monitoring judges by helping them find the proverbial needle in the haystack and not get deluged by the volume of data routinely produced by the typical case-management systems.

In this paper, we explore the application of intrusion detection techniques, such as the statistical anomaly detection schemes, to case management systems and present the results from our extensive case studies. Our proposed system, now in pilot, shows high accuracy in flagging anomalous cases, reduces the overall volume of information generated by the system and can help target several of the key reasons behind case pendency while bringing much needed transparency to the overall case-flow.

1. Introduction

Over the last few years, judiciary in Pakistan, buoyed by massive support from the people, has made significant strides towards providing effective and speedy dispensation of justice to the people. However, a number of problems still need to be addressed in this regard. For example, there is a huge backlog of existing cases which, according to some estimates, is more than 200,000 in one province alone [19]. Unfortunately, similar numbers can be found in comparable contexts where proper court management systems are not in place [20]. The current record-keeping systems are broken; Information Technology is barely used in courts, if at all [14]. Before the advent of electronic databases and other technological tools, managing large quantities of information such as case records included paper notebooks, ledgers, and variously sized wooden cabinets and cardboard boxes filled with paper index cards [5]. In Punjab for instance, case documents are still kept in actual physical binder files that reside in record rooms with double-entry book-keeping to track files from desk to desk as the trial proceeds. Such a system is prone to a wide variety of tampering, misuse and abuse. The lower/district judiciary, in particular, is rife with such problems where a lack of transparency in the system leads to serious delays and pendency. One of the major reasons for this has been a lack of adequate monitoring mechanisms on the part of the superior judiciary.

The institution of a ‘monitoring judge’ from the higher courts to oversee the working of the lower courts was introduced to solve this problem. Currently, the work of inspecting the lower courts is done through ‘Monitoring and Inspection’ teams that solicit monthly pendency reports from the lower courts. Many different requirements can be placed on such a monitoring system. One such requirement is that the system should be effective in making the processes more transparent by helping identify problems that affect a typical case-flow. The current monthly report format provides summary statistics on the number of pending cases in each court at the start of the monitoring period, the number of cases completed and the number of new cases instituted. The process of gathering this data is still largely paper-based which is both time-consuming and prone to errors. Also, this self-reported numeric data presents little or no meaningful information to the monitoring judges in order to judiciously evaluate the performance of the
lower judiciary. Furthermore, with the increasing number of new cases and a huge back-log of existing cases, it is impossible for a monitoring judge to keep track of individual judges, courts or cases.

In this paper, we present original research on the design and analysis of a novel ICT based court-monitoring system that can improve the effectiveness of the monitoring and inspection of lower courts by improving the efficiency, security, and transparency of the processes. The main components of our solution consist of a statistical anomaly detection engine built on top of a case-management system in order to keep an accurate tamper-proof log of a case-flow, reduce the volume of data that a monitoring judge would have to look at, thereby enabling focused interventions and faster responses. Our goal is to facilitate judges and litigants by making the processes more transparent while allowing effective monitoring and improving access to justice.

A typical case-management system that records a fine-grained history of all ongoing case related activity would not be very useful for monitoring. Therefore, we try to focus on mechanisms to facilitate tracking of only key events in a “normal” case time-line. The problem is actually analogous to one faced in typical security systems. If an Intrusion Detection system generates too many alerts, a system administrator will eventually start ignoring the alerts generated by the system[8]. We borrow ideas from intrusion detection schemes to automatically create profiles of normal case-flow. Any deviations from the normal flow can be flagged by the system and potentially be investigated by a monitoring judge. This allows focused interventions and more effective monitoring.

In this paper, we present the findings from our ongoing pilot project in one district in Punjab on the role of IT in improving judicial services. Since the use of ICT related technologies to improve the dispensation of justice is not a novel idea, we present a detailed description of the use of technology from around the world in section 3. In section 4, we describe the data collected to test our system. This is followed by a description of the architecture of our system in section 5. A detailed discussion of the results is presented in Section 6. We conclude the paper with an analysis of our scheme, our future plans and possible extensions to the project.

2. Motivation

Electronic Case Management Systems or (CMS) have been extensively used in the past to help the management of cases [7] in a court. The state of the art systems are not just designed to digitally mimic the functionality of paper-based registers, but introduce functionalities to help monitor the output and performance of the courts. Some of the functions performed by the CMS include the support and automation of the back-office administrative work of court staff, case tracking, case planning, document management and scheduling of hearings etc.

As noted earlier however, while a case-management system is an important tool in expanding the role of IT interventions in court operations, the volume of data generated by the system can be potentially so huge that it is impossible for a ‘monitoring judge’ to actually deduce meaningful conclusions from the data. A back of the envelope calculation can help illustrate this point. For example, each monitoring judge in the Lahore high court is charged with monitoring the lower court judges in at least one district. A typical district court has around 40 judges on average and each judge’s court has around 500 cases on its docket. A fine-grained case-management system, that records all the hearings of a case, generates nearly 3000 new entries per day for an average size district (assuming a daily average of 70 cases being fixed for hearing in a court). If a monitoring judge were to look at his district every week, he would potentially be looking at 15000 entries in order to determine how the lower courts were performing. Clearly, this is not an ideal situation and reduces the utility of a CMS from a monitoring perspective.

In order to be effective, a monitoring mechanism should generate concise, timely, accurate, credible and actionable information that allows us to sift through the huge volumes of court activities’ data. This speaks to the need for a solution that can automatically ignore the normal case-flows and flag only the abnormal activity in the system thereby reducing the enormity of the task and allowing more focused interventions from a monitoring judge.

Actionable intelligence however, requires balancing efficiency with accuracy; a problem that has been studied in detail in computer security literature.[8,12] An important requirement of security systems such as Intrusion Detection systems is that they should be able to: a) detect a very high percentage of attacks, misuse and abuse in the overall system, and b) substantially reduce the overall volume of traffic generated to make sure the system administrators do not get lost in a deluge of data[8].

The overall architecture of our scheme combines a statistical anomaly detection engine with a misuse detection scheme on top of a case-management system in order to provide actionable intelligence on a large volume of cases to a ‘monitoring judge’ in order to enable effective monitoring of lower courts. Instead of having to sift through 15000 hearings per week, the judge could instead pay attention only to the anomalies
thrown up by the system and dig into those cases in more detail.

3. Literature Review

Our literature review for this paper is composed of two parts: a) the use of technology in the judicial setting as an outcome of a trend towards e-governance and e-justice, and b) research on intrusion and anomaly detection and the various practices that have been adopted and are currently in use.

3.1. Judiciary and ICT

ICT related interventions in the judicial system are not a new phenomenon and the world has been moving towards electronic judicial systems and replacing paper based systems since decades [5][9]. The incorporation of ICT into the court setting is a phenomenon that belongs to the emerging realm of e-justice, an integral branch of research in e-governance. “E-justice” has been termed as the application of the “e-government approach” to the judicial sector [4].

Previous interventions in this area have focused on three distinct types of technologies [7]. The first group consists of basic technology such as computers, spreadsheets, emailing facility etc. Such technologies can be found in most court settings across the globe including Pakistan to a certain extent. The second category is composed of technologies to support the activities of the judges, such as law and case law electronic libraries, and sentencing support systems [7].

The third group of technologies that include electronic case management systems (or CMS) facilitate judicial administration and promote better governance through technology. These technologies enable the development of interoperable judicial systems, reduce operational expenses, result in fewer case delays, ease scheduling and assist in the creation of storage and back-ups [5], [6], [7], [9], [10]. Some of the more sophisticated systems produce performance statistics and graphs for the judges [7]. Italian courts have explored the use of barcode readers and optical scanners to track and locate case files [7]. Courts in India have also implemented several interesting ideas in the form of video-taping of all court proceedings, scanning and digitizing all forms of documents and evidence, digital access controls, security mechanisms, web-casting of live proceedings etc. [13]. In the Indian context, some of the future extensions being envisioned include incorporation of OCR (Optical Character Recognition) services, creation of a cloud for e-courts and development of a decision support system for judges [13]. Other active areas include electronic complaint services, process serving, automatic scheduling of hearings and automatically generated messages to relevant parties [9]. Some countries have explored providing web-based repositories of legislation and case law. Several others have explored e-filing of cases and electronically exchanging legal documents [7].

As more and more data and systems are computerized and moved online, there is a growing need to ensure the reliability, accountability, reproducibility, ownership, and accreditation of such data [17]. Provenance or lineage of archival record data such as judicial records etc also becomes critical in determining its validity, authenticity and hence usefulness. Therefore, it is essential for current research to look into establishing security and privacy in the e-court setting and look into the implications and consequences of technology [3], [9].

Pakistan is unique in some sense simply because most of the nuts-and-bolts activities related to the administration of justice, such as, courtroom proceedings, issuance of notices or summons, fixation of cases etc., even at the higher courts level, are unaffected by the latest technology and continue in the forms of old. Lower courts have little or no technology at all. By and large, the processes related to case management are still being done manually. A case file, which goes from desk to desk, is tracked through entries in multiple book keeping registers that are stacking up and occupy a lot of storage space. Such paper-based systems are notoriously hard to monitor and increase the opportunities for corruption by members of the lower staff. Similarly, no IT applications are involved at all when it comes to either the scheduling of court hearing for cases, recording the court proceedings or storing case records electronically for generating authentic copies. Effectively, the role of the IT department staff, if available, has been reduced to typing daily cause list, the occasional orders and sending emails.

3.2 Anomaly Detection

Looking at the intrusion detection literature, typical intrusion detection schemes require that any activity on a node or network is audited and compared to a description of acceptable behavior [2]. Intrusion detection systems (IDSs) can be classified as anomaly detection or misuse detection. Anomaly detection based systems such as IDES [16], model normal behavior based on typical usage patterns using statistical measures and any deviation is considered an attack. Misuse detection based systems such as SNORT etc. model behavior that clearly indicates an attack [15]. The main weakness of such a system is the fact that the system is unable to detect any unknown intrusions. Our scheme combines statistical anomaly detection with rule-based misuse detection techniques.
to automatically sift through the data generated by the case management system in order to identify anomalies, track performance and flag violations of specified policies.

Various statistical and machine learning based schemes have been used in Intrusion Detection systems to reduce the number of false positives, reduce the overall volume of data generated, thereby reducing the computational and storage overhead. The key ideas revolve around using data mining techniques to discover consistent and useful patterns of system features that describe normal program and user behavior, and use the set of relevant system features to compute (inductively learned) classifiers that can recognize anomalies and known intrusions.

4. Research Methodology and Data Collection

While delay and pendency have been widely recognized as two of the most important factors hampering dispensation of justice in Pakistan, to this date, there has been no systematic analysis of court records to substantiate this argument. Justice (r) Hamood-ur-Rehman’s law reform Commission Report from 1967 analyzed a few cases and provided the break-up of the delays that a civil/criminal case may have. As part of a collaborative research effort with the Law and Justice Commission of Pakistan, we studied a large number of cases from multiple courts that were representative of a typical court caseload to identify the main causes of delays in the lower judiciary in Punjab, the largest province in Pakistan. After a careful analysis, various complexities and defects within the existing systems came to the fore.

We started off by selecting representative civil courts from two different districts: Lahore and Multan. Lahore being the largest city in the province, the total volume of cases was prohibitively large for us to consider. Therefore, cases were randomly selected (using a systematic sample with a random starting point) from the daily roster of cases heard during the month of April 2009. In Multan, cases were purposely sampled to consider only those civil cases that were decided during the period April-June 2009.

We identified case-files as the key record keeping mechanism that needed to be studied in detail. Each case is maintained in a case-file that is a complete running log of the case up to that point in time, including all the technical and administrative details about the case, all transactions, evidence and the orders issued by the judges. The case orders are often written by hand and are generally illegible to a layman. In order to make sense of the data, we photocopied the relevant orders from the files and a team of designated lawyers was setup to record the following information for each order present in the order sheet:
- date order passed
- stage of the civil trial
- reason for adjournment
- penalties for adjournment (if any)

At any given point in time, a (civil) lawsuit in the lower courts can lie in one of the following seven potential stages: 1) Filing, 2) Service of summons, 3) Written statements, 4) Framing of issues, 5) Evidence, 6) Final arguments, and 7) Judgment. While this information formed the building blocks of our monitoring system, other information on case history, lawyers and nature of the case etc was also collected during this phase. To our knowledge, this is the most comprehensive study of actual case file related data in Pakistan. While the data collection is still an on-going effort, the results we quote were deduced from the examination of a total of 300 Civil Case files: 222 of those cases were in Lahore and 108 in Multan. It is important to point out that the statistics described below are based on the detailed data obtained from these sample case files, and the judges’ orders contained therein, all of which is much richer information compared to the information available to a ‘monitoring judge’ at present.

Discussion The data suggests that the most significant sources of delay in a civil lawsuit are:
- non-service of summons on defendants
- non-filing of written statement
- non-availability of witnesses
- un-scheduled absence of the presiding officer
- time spent on miscellaneous applications

Table 1. Summary statistics on each case

<table>
<thead>
<tr>
<th></th>
<th>Lahore</th>
<th>Multan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median # of orders</td>
<td>22</td>
<td>10.5</td>
</tr>
<tr>
<td>Trial Length(months)</td>
<td>16.5</td>
<td>4.5</td>
</tr>
<tr>
<td>Longest order sheet</td>
<td>91</td>
<td>65</td>
</tr>
<tr>
<td>Shortest order sheet</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Shortest case</td>
<td>2 months</td>
<td>1 month</td>
</tr>
<tr>
<td>Longest case</td>
<td>9+ yrs</td>
<td>4 yrs</td>
</tr>
</tbody>
</table>

Another key observation is the fact that Multan and Lahore show distinctly different characteristics from each other, and while cases follow a similar stages in each district, there is very little similarity otherwise, both in terms of total trial lengths, time spent in different stages and causes of delays.

The data also shows interesting characteristics as to the amount of time spent in each stage of the case where Lahore has significantly higher delays in service of summons, filing of written statements and the
evidence stages of the case (see Tables 1 and 2). This is the most significant amount of time spent in the processing of a case. Next, we compiled a list of the top 10 orders gleaned from the case files suggesting that non-service of summons to defendants along with un-scheduled absence of the presiding officers accounts for almost 40% of all case adjournments during the life-cycle of a typical lawsuit.

**Table 2.** Time spent on each case in months

<table>
<thead>
<tr>
<th>Stage</th>
<th>District Lahore</th>
<th>District Multan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filing of case</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Service of summons</td>
<td>4.8</td>
<td>2.3</td>
</tr>
<tr>
<td>Filing of written statements</td>
<td>4.9</td>
<td>1.4</td>
</tr>
<tr>
<td>Framing of issues</td>
<td>1.1</td>
<td>0.6</td>
</tr>
<tr>
<td>Evidence</td>
<td>7.0</td>
<td>3.4</td>
</tr>
<tr>
<td>Final Arguments</td>
<td>1.8</td>
<td>0.9</td>
</tr>
<tr>
<td>Judgement and decree</td>
<td>0.3</td>
<td>0.3</td>
</tr>
</tbody>
</table>

In order to identify the different sources of delay, and explain them to our reader, we selected a sample of cases and analyzed their data. The top ten reasons for adjournment are summarized below in table 3.

**Table 3.** Top 10 Reasons for adjournment

<table>
<thead>
<tr>
<th>Reason</th>
<th>District Lahore</th>
<th>District Multan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-service of summonses on defendant(s)</td>
<td>1616</td>
<td>27.7</td>
</tr>
<tr>
<td>Time for arguments/decision of misc. petitions</td>
<td>1320</td>
<td>22.6</td>
</tr>
<tr>
<td>Filing of written statement</td>
<td>984</td>
<td>16.9</td>
</tr>
<tr>
<td>Unscheduled absence of presiding officer</td>
<td>807</td>
<td>13.8</td>
</tr>
<tr>
<td>Non-filing of replies to misc. petitions</td>
<td>402</td>
<td>6.9</td>
</tr>
<tr>
<td>Non-availability of witnesses</td>
<td>274</td>
<td>4.7</td>
</tr>
<tr>
<td>‘Aakhri moqa’</td>
<td>98</td>
<td>1.7</td>
</tr>
<tr>
<td>Making up deficiency in court fee</td>
<td>82</td>
<td>1.4</td>
</tr>
<tr>
<td>Filing of documents/misc. petitions</td>
<td>82</td>
<td>1.4</td>
</tr>
<tr>
<td>Filing of replication</td>
<td>67</td>
<td>1.3</td>
</tr>
<tr>
<td><strong>Total Number of Orders</strong></td>
<td><strong>5840</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Total Case Files Examined</strong></td>
<td><strong>222</strong></td>
<td></td>
</tr>
</tbody>
</table>

4.1 Pilot

We conducted several on-site visits of the lower courts to assess the feasibility of technology based interventions that could help improve the performance of the courts and in particular target some of the major sources of delays and pendency in the system. Our key findings from the technical evaluation of the IT infrastructure are summarized below:

- The lower courts do not have any external interface (web-portal) with the world at large and the higher courts in particular. Since orders are not posted publically and reside with the lower court staff, this leads to potential source of corruption as well.

- In addition, the current case-file based systems are extremely prone to tampering and modification since there is no backup record of the case proceedings. Anecdotal evidence suggests that “accidental misplacements” and “strategic fire” incidents have played a significant role in denying due process to many litigants.

- Overall, it seems that the existing work-flow does not have checks and balances in place and has been designed under the assumption of benevolence or naïveté on the part of the key players. While this might be a workable assumption, it does make the system vulnerable to all sorts of mistakes and opportunistic behavior in the modern world.

Before concluding this section, it is imperative to point out that most of the judicial staff we worked with at all levels was very open and cooperative about the strengths and weaknesses of the existing systems and have been enthusiastically cooperating with us in the visualization and development of a pilot system.

5. System Design Considerations

We designed our system with three essential requirements in mind: 1) a robust and high quality ‘monitoring’ solution that required minimal changes to the existing workflows, 2) sophisticated analytics engine to facilitate remote case monitoring, 3) a robust architecture that could scale to thousands of cases and courts while tracking problems to individual judges, cases and files.

The initial phase of the project involved building a case management system for our model courts. The primary objective in establishing model courts was to create a live, functional template for potential scale-up to other courts in the country rather than showcase all possible IT applications that could conceivably be used in a courtroom setting.
Having done an extensive study of the system, we rolled out our pilot system in different phases in order to make sure we enlisted the requisite support from the stakeholders and got to observe the results of our interventions. In our case, this meant giving up on the most sophisticated solutions in favor of the ones that were simple, scalable and reliable for a large-scale remote deployment. The primary goal we had in mind was to enable and ensure an effective monitoring of the lower judiciary by the ‘monitoring judges’ at the higher courts. During our visits, we also got to observe the court systems firsthand as well as to meet with relevant judicial, administrative and IT staff to understand the actual business processes behind the day to day running. Careful evaluations and discussions with stakeholders and prototype developments helped us get a better insight into a model that might be well appreciated by the end-users.

5.1 Architecture of the system.

As described earlier, the main components of our solution consist of a statistical anomaly detection engine built on top of a case-management system. The case-management system is a web-based client-server application based on PHP and a Mysql database with client-side scripting done through JQuery. The server runs on top of a standard Ubuntu installation. It is important to point out that all the components of the system are essentially open-source and cost nothing in terms of licensing fees and maintenance. The statistical anomaly detection logic is implemented through server-side PHP scripts.

Our case management system provides a platform to the court staff for entering case information and viewing graphical statistics related to the cases in the system. Each lower-court judge is provided access credentials to the system and has a personalized interface which represents his court proceedings. Figure 1 shows a snapshot of the system for a particular judge. While a regular login allows only restricted write-once access to the system, the monitoring judges are provided separate credentials that can be used to access data and information across several courts along with several key performance indicators as described later. The initial case management system was designed to facilitate robust data collection and later extended to include statistical anomaly based flagging of cases along with misuse detection. Further discussion on the case management system however is beyond the scope of this work and instead we focus on the analysis engine which, to the best of our knowledge, is unique in its approach towards generating actionable data analytics from case-flow data.

5.2 Analysis engine

As motivated earlier, an essential requirement for a ‘monitoring’ system is that it should automatically ignore normal case-flows, determine abnormal activity or patterns and automatically alert the supervising judge so that they can dig deeper into problem cases to see why a particular alert has been generated. Such a platform can also double as an effective performance evaluation tool where the performance of judges can be monitored and evaluated effectively across several dimensions including efficiency, quality of judgment etc.

There are two main approaches to intrusion detection ‘anomaly detection’ and ‘misuse detection’ and we incorporated both of the approaches in the design of our analysis engine.

5.3 Statistical Anomaly Detection

The ‘anomaly detection’ engine was built on top of the case management system and was based upon a typical intrusion detection system (IDES) [16]. IDES flags activity that is considered sufficiently deviant from established normal behavior that has been observed in the past. The idea relies on building a profile of normal behavior by instrumenting an application during a training period to calculate average and deviations statistics for most normal activities such as file I/O, network I/O, system calls etc. The system can subsequently flag as anomalous any behavior that is not within a threshold of the normal profile. Also, anomaly based schemes require no prior knowledge of what abnormal behavior would be like. Heavier training during the learning phase with known normal behavior reduces the probability of normal behavior generating a false flag. Simultaneously, this increases the likelihood that a new behavior will get flagged (since the system’s notion of normal is more closely associated with the known behaviors).
We modeled each case as a state diagram with the states representing the actual stage of a case and the transitions representing the actual time it took for a case to move from one hearing to another and possibly to a different state. With this in mind, we chose a representative sample of three months of civil cases from our model district as a training set. Data from our previous research into case-files (see Table 2) strongly suggested discernible patterns in cases that could be used to create a normal profile. We also noted that the times-lines of a case also differed significantly from each other based on the type of the case. For instance, a family case follows a very different time-line as opposed to a property dispute, often necessitated by law.

Once the training set was selected, each case from the training-set was analyzed by our analysis engine as it was being entered to create a normal profile for each type of case. The normal-matrix, as we call it, is a 7x7 matrix where the columns and rows represent the seven different stages in a case. Since each hearing in the case-management system is time-stamped, each entry $[i,j]$ in the matrix represents: a) Frequency of transition (no. of times this transition has occurred from stage $i$ to $j$) b) Mean and Std. Dev. time in stage $i$ before transition to stage $j$ c) The probability of transition from stage $i$ to $j$ which essentially is frequency $(i,j)$ / Sum of frequency $(i,k)$ ($k$ goes from 1 to $n$).

Once the training period is finished, the run-time environment takes over. As a new hearing’s data is entered into the system, the analysis engine automatically marks and flags a case if the hearings fall outside a tunable threshold of the statistics available in the normal-matrix. As noted earlier, each type of case, in each district (as shown in the datasets from Lahore and Multan) and perhaps even each judge has a different notion of what the normal matrix is like and each of these statistics can be individually maintained by the system. Also, a monitoring judge can easily tweak these threshold values through an admin interface.

Similarly, the system is capable of flagging other anomalies such as unusual transitions from one stage to another. If the case jumps from a state to another state where the corresponding probability of transition is zero (or below a certain threshold), the system can automatically flag the case. This feature can potentially help reduce arbitrary decision making by the judge who would now be forced to follow procedure since any violations would be flagged by the system.

5.4 Misuse Detection

The second part of the analysis engine is the ‘misuse detection’ component. Several well-known intrusion detection systems have been built upon creating rule-sets for misuse detection. Popular IDS systems like Snort[15] allow administrators to setup their own arbitrary rules that are applied on all incoming traffic. While the detection rates for this kind of detection are really high, the major shortcoming is that the system is confined to detecting only previously known threats.

In the judicial context, several policy guidelines are laid down by the Law and Justice Commission (LJCP) in order to expedite certain cases or provide preferential treatment to certain types of cases. For instance, the current policy guidelines suggest disposing off family related cases (divorce, custody of minors, guardianship, succession etc) within six months. Similarly, the policy suggests disposing off rent related cases within four months and all writ petitions, appeals related to them within 6 months.

The simplest example of such a rules is to flag a custody case that has not been decided inside of 6 months. Another possible rule would be to check if a case has been adjourned for more than $x$ hearings due to the presiding officer not being present. The system allows the monitoring judge to setup these rules on the fly and the tweak the arguments. The underlying system can then automatically flag any cases in the system if any of the stipulated rules are violated.

5.5 Discussion

Security systems often require users to craft a normal and/or anomaly profiles by hand thus making the system unusable for anyone but the most sophisticated user. The anomaly detection part of our scheme automatically creates the rule-sets without burdening the end-user. The down-side of using such a scheme though, is the notion of false-negatives (abnormal behavior not flagged) and false-positives(normal behavior wrongly flagged). This is not a huge issue in our system since we only use our engine to flag anomalous data to help a monitoring judge hone into a more concise set of cases rather can get deluged by a whole flood of case data. The underlying data still gets recorded for every hearing and more sophisticated techniques can later be applied on the data to analyze it.

The scheme adopted for flagging anomalies is a simple yet powerful idea, several successful intrusion detection algorithms have been built on similar concepts[15]. Our pilot system successfully demonstrates the use of such schemes to automatically sift through large volumes of data. However, we note that there are several more advanced schemes that can be explored the mine the case-data collected.
6. Testing and Results
To evaluate our monitoring architecture, we developed all the components that allowed us to gather data from real court rooms and workloads. The court-management system was setup in two courts in our model district. For simplicity, we only looked at civil cases as a start but note that criminal cases follow similar state-transitions, timelines and procedures.

The resulting system tracks a case from the moment it gets marked to a particular lower court and tracks its life-cycle through a series of order/action summaries capturing court activity on the dates that the case gets presented before the court. No effort was made to record any other information related to the case including evidence etc. The interface for the case management system was kept simple enough to keep the number of “clicks” to a minimum. This was done keeping in view the limited exposure of the court staff responsible for entering the data into the system.

Both our model courts had a docket of almost 500 cases with the oldest cases being around 5-6 year old. This involved an extensive effort into coding and entry of the extended prior case history into the system. During a preliminary analysis over a one month period, we found out that on average, the system was generating almost 1500 new entries per court. The training dataset was chosen by randomly selecting 200 cases from the existing dockets per court. This training dataset was used to create normal profiles for each type of case.

The first set of experiments was conducted to figure out if different types of cases were significantly different from each other for a given court. There were 4 different types of family cases for a total of 80 in our training dataset; A) dissolution of marriage, B) dowry settlement, C) maintenance and D) custody of minors. Once the normal profiles for all four types of civil cases were created, we tested it against the remaining 100 to see if the system was able to classify them correctly according to the type of case. As it turned out, the system was able to classify them as family cases with an accuracy of around 95% in both normal and testing workloads. Among the family cases, dissolution of marriage and custody of minors had an accuracy of 90% and 85% respectively. Dowry and Maintenance were classified correctly only 82% of the time. While the numbers were really encouraging and the system was able to identify types of cases based on the data with a high degree of accuracy. We note that the accuracy of detection was negatively affected due to the small training datasets. Heavier training with normal data would improve the accuracy of detection further.

The second set of experiments was done by artificially introducing random delays into the testing dataset. The ‘tunable’ threshold for flagging cases was set at 1.5 deviations from the average delay for any particular stage. The system was able to successfully flag the anomalies above the threshold with a low false-positive rate (4.5%). We believe this is a fairly decent false positive rate and does not introduce too much extra data for a ‘monitoring’ judge. A judge can discard these false alarms by clicking on the case-file and checking to see why the system has flagged the case.

Since the prototype system is already in pilot, we are planning to run an extensive set of experiments in the coming weeks to further test the accuracy of the detection, establish better profiles for normal case-loads and setting up better misuse detection rules through an active collaboration with the research wing at the higher courts.

7. Limitations and Future Work
The value of any decision support system is essentially in the quality and provenance of the data being input to the system. A quick analysis of the access-control credentials of the users confirmed our fears that the current password based authentication system becomes the weakest link in the data provenance chain. Most of the passwords being used in the system are simple enough to guess and brute-force. While our data-base servers do restrict access to a small subset of court IP addresses, we see weak passwords as a major limitation of the system. We are currently exploring biometric authentication schemes to add non-repudiation and authentication to the system.

Another major shortcoming of the system is the fact that most of the data used for the analytics is self-reported. While there is an incentive to cheat the system, we note that if the court-staff does input falsified information into the system, the case-file and the permanent online record would no longer be in sync. Our current prototype does not provide access to the litigants. If the litigating parties could potentially point out the discrepancies at any point, there would be little incentive to try to cheat the system since the consequences could be severe. However, right now, our system does not provide this functionality. We note however that an sms-based solution that updates the litigants about daily summary proceedings as recorded online can be easily appended to add transparency to the system.

Another major stumbling block is the nature of the pilot project. We have very limited visibility into the life of a typical case-file. A case can get transferred from between lower courts or to a higher court even across districts. Similarly, judges can change or get transferred creating problems for the system. Since we are only targeting one district, our visibility into a
case’s history is only limited to a particular court or district, once a file moves out of the system, there is very little we can do in terms of monitoring till it comes back to our pilot courts. With a universal deployment, such end-to-end issues can be mitigated. A related issue was identified when we went to a new court to add it to the pilot. Since the system relies on the whole docket being entered into the system, this requires manually going through case-files which are often hundreds of pages thick and trying to identify the key information elements that need to be entered into the system. We realized very quickly that the case-file was illegible to most of our research team adding significant delays to our system. The writing was often scribbled and smudged and only a trained eye could make sense of most of the documents. We are currently handling the problem by hiring specialized data-entry operators, recruited from the retired court-staff who are assisting us in deciphering much of the case files.

We strongly feel a case monitoring system and analytics are an interesting area of research, however, being in a less-developed country setting brings up a unique set of problems each of which we see as an opportunity for future work. Due to the low computer literacy in most of Pakistan, we are continuously trying to reduce the total number of clicks a courtroom official has to make to record information in our system for each hearing. This was one of the major stumbling blocks since the lower staff was unable to follow the sequence of instructions correctly if the number of clicks per task was large. A combination of drop down boxes, templatized orders and more intuitive graphical interfaces is currently being explored to further reduce the learning and operational overheads for the court staff. Our team has also produced a step-by-step user-manual in the local language in order to reduce the learning curve for the court-staff and the feedback has been excellent. As a followup we are currently preparing workshop materials and tutorials in order to help facilitate quick adoption. It would be important to reiterate here that by and large, we have received excellent cooperation from the staff who are genuinely interested in working with us.

A relatively low-hanging fruit is a bar-code reader based file tracking system for case-files. Integrated with an anomaly detection system, this could be useful in tracking if a file was spending too much time on one desk without being forwarded. We are planning on incorporating this in the next iteration of the system.

Fixation of hearing dates is one aspect of the system which is still completely arbitrary. By allowing automatic fixation of dates for cases, the process of hearings for individual cases can progress in an efficient and timely manner thereby avoiding unnecessary and arbitrary delays. The application would be able to check for available slots in a judge’s calendar and give a date for the next hearing. An additional key feature of an automatic date fixation system could be that it would allow all cases of the same category to be dealt with in a continuous time slot. This would organize the daily schedule of the judges and result in a more efficient and productive day. We are currently exploring this design space with our partners in the judicial service with a view of coming up with a workable solution.

8. Conclusion

In this paper, we postulated that a major reason for pendency and delay within the lower judiciary in Pakistan is the lack of an effective monitoring infrastructure. The use of information technology in courts was recommended to help achieve these objectives. However, we feel a case-management system is a necessary but incomplete step towards this goal. Our experience with pilot deployment showed a deluge of data being generated by case-management software leading to a loss in effectiveness. We present a novel use of a threshold based statistical anomaly detection scheme in order to reduce the volume of data generated and allow a ‘monitoring judge’ to hone in on the exact causes of anomalies, i.e. delays, in the system. This would allow the monitoring judge to better utilize their time and, in turn, would make the performance of the courts more predictable and less vulnerable to abuse.

In light of our results, we have argued that a court automation system has to come with an effective data filtering mechanism in order to be useful. Not only would that afford greater control and oversight over the court affairs by making them more transparent for the presiding judge as well as the monitoring judge, our scheme is also expected to improve the experience of the general public.

13. Acknowledgements

We would like to thank Hon. Justice Jawwad S. Khwaja and Hon. Justice Syed Mansoor Ali Shah for encouraging us to undertake research on this topic and their impetus and leading role in its conceptualization and execution. We are also grateful for their contribution of resources to this project and for the tremendous assistance provided by the wonderful folks at Technology for the People Initiative(TPI).

14. References

[1] National Judicial Policy, Pakistan, 2009

[2] Steven Hofmeyr, Stephanie Forrest, and Anil Somayaji,


[9] Harvard Journal of Law & Technology Volume 26, Number 1 Fall 2012 Using technology to enhance access to justice Section author: access to justice integration with emerging Court technologies (James E.Cabral & Thomas M.Clake)


[18] National judicial commission report, Pakistan, 2010