A crime data analysis framework with geographical information support for intelligence led policing

Mahawaga Arachchige Pathum Chamikara, Akalanka Galappaththi, Roshan D Yapa, Ruwan D Nawarathna, Saluka Ranasinghe Kodituwakku, Jagath Gunatilake, Liwan H Liyanage

The manual crime recording and investigation systems in police stations all around the world are generating piles of crime documents which make storage and retrieval of reliable crime information extremely difficult as well as inefficient. Furthermore, investigators of central authorities have to manually search through these documents and communicate between the relevant police stations to obtain required information. Eventually, delays in information flow between investigators of crime incidents cannot be avoided. Sri Lanka Police too have been facing the same set of issues over many years. To get rid of pilling of large number of documents annually in police stations, Sri Lanka Police is allowed to destroy the documents related to solved crimes which are older than five years. This may destroy not only "closed files", but also very valuable information that can be used in future crime investigations.To overcome this problem, this paper proposes a web-based framework with geographical information support which contains a centralized database for crime data storage and retrieval. Geographical capabilities of the framework support not only spatial analysis but also provide an efficient solution to current manual crime map generation. Our highly secured and user friendly framework follows the state of the art layered architecture which provides an optimized data model for fast access and easy analysis of crime data. The solution consists of an affluent set of data mining tools which are essential in any crime investigation process. Security of data is ensured with data encryption for sensitive information and by limiting access to the data through a role based access method. Further the data is only accessible through a virtual private network (VPN) connecting all the police stations and other relevant departments of the Police. The proposed framework was evaluated by conducting an experimental study and the results are promising.

PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

A crime data analysis framework with geographical information support for intelligence led policing

M. A. P. Chamikara[1, 2*], A. Galappaththi[1], Y.P.R.D. Yapa[1, 2], R.D. Nawarathna[1, 2], S. R. Kodituwakku[1, 2], J. Gunathilake[1, 3], L.H. Liyanage[4]

[1]Postgraduate Institute of Science, University of Peradeniya, Sri Lanka,

[2]Department of Statistics and Computer Science, University of Peradeniya, Sri Lanka,

[3]Department of Geology, University of Peradeniya, Sri Lanka,

[4]School of Computing, Engineering and Mathematics, University of Western Sydney, Australia.

Corresponding author:

M.A.P. Chamikara,
No.22, Nikaketiya, Menikhinna, 20000, Sri Lanka
Email address: pathumchamikara@gmail.com

Abstract

The manual crime recording and investigation systems in police stations all around the world are generating piles of crime documents which make storage and retrieval of reliable crime information extremely difficult as well as inefficient. Furthermore, investigators of central authorities have to manually search through these documents and communicate between the relevant police stations to obtain required information. Eventually, delays in information flow between investigators of crime incidents cannot be avoided. Sri Lanka Police too have been facing the same set of issues over many years. To get rid of pilling of large number of documents annually in police stations, Sri Lanka Police is allowed to destroy the documents related to solved crimes which are older than five years. This may destroy not only "closed files", but also very valuable information that can be used in future crime investigations.To overcome this problem, this paper proposes a web-based framework with geographical information support which contains a centralized database for crime data storage and retrieval. Geographical capabilities of the framework support not only spatial analysis but also provide an efficient solution to current manual crime map generation. Our highly secured and user friendly framework follows the state of the art layered architecture which provides an optimized data model for fast access and easy analysis of crime data. The solution consists of an affluent set of data mining tools which are essential in any crime investigation process. Security of data is ensured with data encryption for sensitive information and by limiting access to the data through a role based access method. Further the data is only accessible through a virtual private network (VPN) connecting all the police stations and other relevant departments of the Police. The proposed framework was evaluated by conducting an experimental study and the results are promising.

Introduction

Increasing trend of grave crimes in a society indicates that the security agencies have to shoulder the burden of criminals in larger numbers than the past. A considerable number of criminals has already been convicted and imprisoned; some of them have been released after completing their imprisonment and released under supervision, while many criminals are committing their activities inside the civil society without being caught. This perpetual trend has made the process of investigating crimes very complex. Sri Lanka Police too has been facing with these difficulties for a long time. According to statistics, on average, 52000 grave crimes are reported annually in Sri Lanka [1]. Once a crime is reported, it is recorded and investigated by the relevant legislative police station of the particular area.

According to the penal code first enacted in 1882 and amended subsequently several times in later years [2], crimes are classified into two categories: Grave crimes and Minor offences. Until 2014 grave crimes were classified under 21 categories and in 2015 another 5 new crime categories were introduced by making it 26 categories of grave crime types. Table 1 shows the 26 crime types and their corresponding Penal codes/ Sections.

Table 1. Grave Crime Types of Sri Lanka

No	Crime Type / Offense	Penal Code/ Section
01	Abduction	354-360
02	Kidnapping	355-360
03	Arson and mischief	418,419,421
04	Fraud or mischief causing a damage greater than 25000 rupees	410,417,420,426
05	Burglary	440-446
06	Grievous hurt	316,317
07	Hurt by sharp weapon	315
08	Homicide	296,297
09	Attempted or committed homicide	300,301,299
10	Rape (above 16 years of age)	364(1) 364(2) 364(ඇ)
11	Statutory rape (below 16 year of age)	364(1),364(2), 364(3), 364(ඇ)
12	Unlawful assembly and riots	140-149
13	Robbery	380-385
14	Unnatural offence	365, 365(ඇ), 365(ආ)
15	Extortion	318,373,378
16	Cheating with trust	386,387, 389, 392 (ආ), 400-403
17	Theft	367,368, (ඇ),(ආ), 369, 370, 394, 396
18	Counterfeiting and forging currency	226,246
19	Offense against state	114-126
20	Child cruelty	308,308 (ඇ)
21	Child sexual abuse	360 (ආ)
22	Human trafficking	360 (ඇ),360 (ඈ)
23	Offensive weapon act	1966 act number 17
24	Use of automatic or repeater guns	Section 22(3) of 182 act number of weaponry authority revised with

PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

		Section number 13 of 1996 act number 22.
25	Using dangerous drugs	Section 54(ඇ) and 54(ඈ) which is read along with 1986 act number 13 of 3rd schedule of 218 authority.
26	Obstruction to duty	183

The crime recording and investigation process along with the court process involves a great amount of data recording, data retrieving, and the investigation is extremely difficult and time consuming with piles of manual documents.

Increasing population, increasing income gap, complex social and political needs have made the path for most of the crimes today [3]. By considering the complexity and the increasing number of crimes, it is very essential to use advanced data analysis technologies for crime investigations and crime prediction. Data mining and decision support systems play a major role in crime analysis [4]. Data used for collaborative solutions must be standard in order to achieve accurate and precise results. It is a prime step to properly organize the current and past paper-based crime data in electronic databases to support future crime investigations. For example, serial criminals are regularly updating and changing their modus operandi and also use multiple identities [5]. Investigation of such crimes need closer look at similar crimes taken place in past and correlations between them to find the culprits. Finding the most suitable model can still be situational due to the rational, dynamic criminal behaviour and dynamic nature in criminal organizations [6].

To overcome the above limitations a novel scalable crime investigation framework for intelligence led policing is proposed, named “Sri Lanka Crime Investigation Decision Support System” (SL-CIDSS). The proposed system is a web based intelligent crime analysis system with GIS (geographic information systems) support. The system comprises of data mining tools in support of efficient information extraction and crime analysis from historical and current crime data. SL-CIDSS is a distributed crime analysis system with a set of crime analysis tools which includes the PostgreSQL database server. PostgreSQL is an open source relational database management system (DBMS) [7]. SL-CIDSS provides spatial analysis features with the incorporation of PostGIS extension [7] into the PostgreSQL database. Crime locator, Crime clock, Periodic pattern visualizer, Crime map, Hotspot detection, Nearest police station detection, Crime comparator and Modus Operandi analysis are some of the very important crime analysis tools available in SL-CIDSS.

The rest of the paper is organized as follows. Related Work and Background section presents a summary of the work that has been done on crime data recording and analysis as well as a brief discussion on crime data analysis tools in general. Materials and Methods section discusses the requirement analysis, design and implementation approaches and each of the important components of SL-CIDSS in detail. Next, Results and Discussion section provides a performance evaluation of SL-CIDSS, improvements over the previous version of SL-CIDSS (i.e., SL-

SecureNet), and some user feedback. Finally, some concluding remarks and future enhancements are outlined in the Conclusion Section.

Related Work and Background

Literature shows several systems implemented to achieve the task of crime data integration and investigation. COPLINK is one of those systems which has incorporated a collection of data mining tools to support the investigation process of Tucson police department, USA. COPLINK provides an easy-to-use interface that integrates different data sources such as incident records, mug shots of criminals and gang information, and allows diverse police departments to share data easily [8]. Uniform Crime Reporting: National Incident-Based Reporting System [9] is an automated information system which has aimed at providing reporting standards which are oriented towards enhancing the quantity, quality and timeliness of crime statistical data collected by the law enforcement community and improving the methodology used for compiling, analysing, auditing, and publishing the collected crime data .

TAS (Timeline Analysis System), AICAMS project, FALCON (Future Alert Contact Network), and CCHRS (Consolidated Criminal History Reporting System) are some of the systems which serve as information management or intelligence analysis tools for law enforcement. Each of these systems has their own advantages as well as drawbacks. One of the main drawbacks is the unavailability of a complete knowledge base [8]. Eventhough there are several live crime information systems available, they are custom made for legislative authorities in different countries and those systems are not accessible outside of those respective authorities. CrimeReports online system [10] is one such automated system. Carson et.al have developed a web-based crime analysis toolkit designed especially for Virginia law enforcement agencies, in United States, called WebCAT 2.2 with improved data sharing capabilities compared to their previous versions [11]. They introduce the data sharing, analysis, mapping, and querying capabilities which are not available in the crime mapping and analysis software programs: such as Rigeel, CrimeStat III and Dragnet where crime mapping refers to mapping, visualization and analysis of crime incidents with the help of geographical maps. Most of these systems are expensive [11], not easily customizable to different domains of legislation and do not provide a complete knowledge base.

Clustering crimes, finding links between crimes, profiling offenders and criminal network detection are some of the common areas of data mining applied in crime analysis [12]. Association analysis, classification and prediction, cluster analysis, and outlier analysis are some of the traditional data mining techniques which can be used to identify patterns in structured data. On the other hand, new data mining techniques help identifying patterns in both structured and unstructured data [4]. The concept-space approach has been used in COPLINK project to extract criminal relationships from incident summaries and has created a likely network of suspects by measuring the co-occurrence weight of two criminals. Single link hierarchical clustering has been used to partition the network into sub groups and block-modelling approach has been used to identify the interaction patterns between the subgroups.

Centrality measures such as degree, betweenness, and closeness have been used to detect the key roles in each group, such as leaders and gatekeepers [13]. K-core method is one of the most common methods used in Social Network Analysis (SNA) [12]. Furthermore, affinity propagation and Bayesian networks can provide promising results in identifying relationships between entities and structure of the network [6], [14]. Offender profiling is a methodology which is used in profiling unknown criminals or offenders. There are several other synonyms such as criminal profiling, criminal personality profiling, criminological profiling, and behavioural profiling which are used to refer to the same concept. The purpose of offender profiling is to identify the socio-demographic characteristics of an offender based on information available at the crime scene [15]. Entity extraction is a technique used to identify the specific patterns in text, image, or audio data. Entity extraction mainly helps in identifying behavioural patterns of serial offenders [4]. COPLINK uses named-entity extraction which is a modified version of AI entity extractor system [16]. It uses three steps to identify the names of persons, locations, and organizations in a document. Step one is to identify the noun phrases according to linguistic rules. Second step is to calculate a set of feature scores for each phrase based on pattern matching the lexical lookup. Step three uses a feed forward/back propagation neural network to predict the most likely entity type for each phrase [4]. Clustering techniques are applied to group crimes or offenders in to classes with similar characteristics. For example, this technique can be used to identify the criminals or gangs who do the crimes in a similar fashion, who have common interests and same person with multiple false identities. Clustering techniques are more effective in crime association detection and prediction which is useful in finding related crimes with similar features. Complete-link algorithm, single-link algorithm, k-means algorithm, self-organizing maps and affinity propagation are some examples for cluster techniques [4].

Association rule mining discovers the items in databases which occur frequently and present them as rules. Since this method is often used in market business analysis to find which products are bought with what other products, it can also be used to find associated crimes conducted with what other crimes. Here, the rules are mainly evaluated by the two probability measures, support and confidence [17]. Association rule mining can also be used to identify the environmental factors that affect crimes using the geographical references [18]. Incident association mining and entity association mining are two applications of association rule mining. Incident association mining can be used to find the crimes committed by the same offender and then the unresolved crimes can be linked to find the offender who committed them. Therefore, this technique is normally used to solve serial crimes like serial sexual offenses and serial homicide [19]. Entity association mining/link analysis is the task of finding and charting associations between crime entities such as persons, weapons, and organizations. The purpose of this technique is to find out how crime entities that appear to be unrelated at the surface are actually linked to each other [19]. Attribution can be used to link crimes to offenders. If two offences in different places involve same specific type, those may be readily attributed to the same offender [12].There are three types of link analysis approaches, namely Heuristic-based, Statistical-based and Template- based link analyses [19]. Sequential pattern mining is also a similar technique to association rule mining. This method discovers frequently occurring items from a set of transactions occurred at different times [4].Deviation detection detects data that deviates significantly from the rest of the data which is analysed. This is also called outlier detection. This is used in fraud detection [4].

In classification, the data points will be assigned to a set of predefined classes of data by identifying a set of common properties among them. This technique is often used to predict crime trends. Classification needs a reasonably complete set of training and testing data because high degree of missing data would limit the prediction accuracy [4]. Classification comes under supervised learning method [19], which includes the methods such as Bayesian models, decision trees, artificial neural networks [20] and support vector machines. String comparison techniques are used to detect similarities between the records. Classification algorithms compare the database record pairs and determine the similarity among them. This concept can be used to avoid deceptive offender profiles. Information of offenders such as name, address, etc. might be deceptive and therefore the crime database might contain multiple records of the same offender. This makes the process of the determination of their true identity hard [4].

SL-SecureNet: Previous Version of SL-CIDSS

SL-CIDSS is a successor of a previously implemented crime mapping system named SL-SecureNet [21]. SL-SecureNet mainly emphasizes on crime mapping. Fig. 1 shows the underlying architecture of SL-SecureNet. When a user sends a standard web request to the system using a web browser, the request is directed to the particular logic through the controllers. The geographical maps are rendered using OpenLayers API (Application Programming Interface) which is an open source JavaScript library to load, display and render maps from multiple sources on web pages [22]. Geoserver [23] is used as the middleware which renders Web Feature Service(WFS) and Web Map Service (WMS) layers of maps composed of crime points. WMS is a specification which outlines communication mechanisms allowing disjoint software products to request and provide preassembled map imagery and WFS is a protocol which allows clients to request map based data as vector data [24]. The Map Layers which are rendered through Geoserver are then displayed together using OpenLayers. A MySQL database is used to store the data of the two data mining tools; nearest police station detection and hotspot detection. The primary data storage was the PostgreSQL database, which is capable of storing geography information. SL-SecureNet was composed of tools such as Crime Mapping, Crime Comparison, Crime Clock, GIS Crime Outbreak Visualizer and Nearest Police Station Detection tool. All of these tools were literally connected to crime mapping. But SL-SecureNet supported only crime mapping and related tools based on summarized count statistics of crime data. Though SL-SecureNet provided a good solution for the manual crime mapping system**,** it didn't support the complete process of crime recording, crime investigation and maintenance of court progress records. Further, the Graphical User Interface (GUI) was not very user friendly. These problems lead to the necessity in extending SL-SecureNet to a more sophisticated system. As a result of that SL-CIDSS was invented.

Fig. 1. Architecture of SL-SecureNet. The controllers implemented in the Spring MVC framework direct the standard user requests to the corresponding logic. OpenLayers API is

used in rendering the maps. Geoserver works as the middleware which facilitates WFS and WMS services in generating the map layers. The PostgreSQL database works as the primary data storage of SL-SecureNet. A MySQL database is used to store the data of the integrated data mining tools.

Materials and Methods

This section discusses the materials and methods used in implementing SL-CIDSS. It also provides the information about the Development approach of SL-CIDSS, The existing crime investigation system, The court processing system of the manual system, The underlying framework of SL-CIDSS and its facilities, GIS capabilities of SL-CIDSS, Enhanced layered functional independency of SL-CIDSS, Information Access and Data Retrieval of SL-CIDSS, Information Security of the framework, Role-based access control model of SL-CIDSS, and Integrated Data Mining Tools of SL-CIDSS.

SL-CIDSS provides an improved version of its predecessor, providing a robust framework having more capabilities with the introduction of 64 entities with over 250 CRUD (Create, Read, Update, Delete) operations, more security with data encryption and improved user role access control and system auditing, more efficiency with data indexing and AJAX, more usability with the improved graphical user interface and help guidance, and an improved collection of data mining tools. Fig. 2 depicts the element interaction of SL-CIDSS in which the police officers can access the tools and reports through a web browser from any police station, through an http based AJAX request which is generated with AngularJS API [25]. If the user is trying to access a map related tool, the request to that tool will be generated with both OpenLayers API and AngularJS API. As the system is accessed through a VPN, it will only be open to the VPN users. When an HTTP request comes to the SL-CIDSS Server, it will be passed to the corresponding controller.

Fig. 2. Main elements and their interactions of SL-CIDSS. Police officers from any police station can access the tools which are facilitated by SL-CIDSS through the VPN. AngularJS and OpenLayers APIs are used in generating a tool related or a map related AJAX request. The system is accessible only through a VPN. SL-CIDSS runs in a web server installed in a server computer located in the Police Headquarters. SpringMVC works as the base framework for SL-CIDSS. SL-CIDSS data model includes the PostgreSQL database with GIS capabilities enabled using the PostGIS extension. System.log is an external file which logs all the system activities in textual format. The database is replicated and the backups are generated once per day.

A controller will pass the request to a particular SL-CIDSS Crime Analysis tool or report which accesses data from the SL-CIDSS Data model through the security layer which encrypts and decrypts sensitive fields of information corresponding to entities such as crime_record and suspect/accused. This is to increase the privacy of data. The data is accessed through the Hibernate Object Relational Mapping (ORM). PostGIS extension has been integrated with PostgreSQL database to work with GIS enabled information. The database is replicated in an external server apart from the SL-CIDSS server located in the police Headquarters. Timed automatic backups are generated to face any contingency in an easy manner. A system log which captures all the actions performed upon SL-CIDSS is generated to record all the user activity to increase the Non-Repudiation of SL-CIDSS.

Fig. 3. Main module arrangement of SL-CIDSS. SL-CIDSS functionalities/services are divided in to modules and related modules are grouped. Each module group is colored using the same color. For example Data Control Module, Data Management Module and Data Administration Module are colored with orange color because the Data Control Module comes as two modules namely Data Management Module and Data Administration Module.

SL-CIDSS framework is based on many web based technologies which provide a layered architecture with room for extension. The layered architecture facilitates to add new entities which reflect the database relations, new services and new visualization API on demand. SL-CIDSS also facilitates online crime mapping, recording, analysing and viewing, hotspot detection, modus operandi analysis, etc., allowing each of the police stations to link with the system. Fig. 3 depicts the main module arrangement of SL-CIDSS. The Figure majorly emphasizes on the arrangement of the modules of functionalities/services provided by SL-CIDSS. SL-CIDSS core module is composed of three main modules of functionalities, namely, Data Control Module, Data Mining Module and the GIS Module. Crime data is stored in the Data Module. The Security Module encapsulates data of the Data Module by incorporating security and privacy concerns. Basically, SL-CIDSS Core Module runs upon the Data Module. Data Control Module is separated into two main modules, namely, Data Management module and Data Administration Module. Conditional crime data recording and analysis are handled by the Data Management Module utilizing CRUD elements. Data Administration Module concerns with the CRUD elements related to the entities with administrative data which are mostly static and must be subjected to more security privileges compared to conditional data. One of the key modules in SL-CIDSS is the Data Mining Module. General Data Analysis Module and the Advanced Data Analysis Module are the two main modules of the Data Mining Module. General Data Analysis Module provides a collection of analysis tools such as Crime Clock, and Crime Comparison which provides the statistics based on crime frequencies. Advanced Analysis Module includes the tools such as Modus Operandi Analysis, Nearest Police Station Detection, and Crime Hotspot Detection, directly supporting the crime investigation process. GIS capabilities offered in the GIS Module of SL-CIDSS allow the system to work with any GIS related analysis such as Geographical Criminal Profiling, Crime Hotspot Detection, Location based crime pattern identification, etc. The outputs of SL-CIDSS are presented by The Reporting Module. It is achieved through the Analysis Reporting Module and the Administrative Reporting Module. The Analysis Reporting Module is responsible for creating reports from the results generated by the Data Mining Module. Administrative Reporting Module deals with reports such as Summary Reports, Annual Progress Reports, Station Progress Reports, etc.

Development Approach

Requirement gathering and analysis was conducted using several software engineering practices, such as observing the existing manual file system; conducting field visits; interviewing the police officers by using top-bottom and bottom-up approaches; conducting group meetings to identify the functional and non-functional requirements and so on. The development process has undergone continuous code walk-troughs to confirm the requirements are satisfied. SL-SecureNet which is the predecessor of SL-CIDSS was used as a prototype to clear the vague requirements. The evolutionary prototyping process model [26] was used for the requirement resolving and system development process of SL-CIDSS. As Sri Lanka Police has been evolving for more than 100 years, the manual crime recording and investigation system is composed of many complex and vague requirements. Prototyping helped in increasing the level of user involvement from the beginning of the development process and to reduce the risks by discovering the technical and other problems early in the process.

Current Crime Investigation System and Court Process

Fig. 4 illustrates how manual crime recording and investigation process of Sri Lanka Police is conducted. As shown in Fig. 4, crime complaints are lodged either by a police officer or by a person anonymously or with his/her identity. If the complaint is about a grave crime the complaint is recorded in the grave crime record (GCR) book. After a grave crime is recorded, investigation is commenced. The crime place is then protected and is visited by the Scene of Crime Officers (SOCO) for collecting scientific evidence and specialist investigations. Crime properties are seized and preserved for further investigation as evidences. Meanwhile as a crime visualization technique and patrol planning technique each police station maintains a *Crime Map* and a *Crime Clock* as depicted in Figs. 5 and 6. Sri Lanka Police daily publishes a Police Gazette, namely PGIII that lists all the crimes and related information taken place within the last 24 hours and send it to all the police stations in Sri Lanka for their information and vigilance. This helps them to capture the criminals and recover crime properties from different police divisions. Identified suspects are detained, questioned and produced before a magistrate within 24 hours of detention. If needed, suspects are produced for an identification parade. The Sri Lanka Police collects relevant scientific analysis reports from corresponding departments and organizations. Required information is regularly updated under the respective GCR number and the crime is reported to a Magistrate at the respective court.

Fig. 4. Flow of events in the Manual crime recording and investigation and court processing system. Double lined elements are the major entities. Single lined entities are the activities carried out under each major entity and the entities with dashed lines represent transient objects which are corresponding to either an input or an output instance.

Charge sheets are produced with advices from the attorney-general. Evidences are processed along with information of the specialist evidences and the prosecution is continued. At the end of a prosecution the judgement is published. The judgements are recorded under six categories, namely B1- False Information Reported, B2- Intentional False Accusation, C1- A Complaint solved with an accused being punished, C2- Suspect being freed with accusations, C3- No Accused, C4 -other. After an accused being sentenced, convicted criminals are registered under Registry of Criminal Records (RC) and Island Registered Criminal (IRC) list and the lists are accessible for interested parties.

Crime map and crime clock generations are two of the critical steps of the crime investigation process as shown in Figs. 5 and 6. All the 41 main divisional police stations draw manual crime maps as shown in Fig. 5 demarcating the geographical area of jurisdiction. The crimes are marked using colored circular annotations. The colors represent different crime types. For example, red color represents homicides. This manual crime map generation is a major drawback of the manual system.

Fig. 5. A manually drawn crime map. A map corresponds to a particular area of jurisdiction. Colored circular annotations represent different crime types. For instance, red , blue, black and yellow are used to denote homicide, burglary, theft, and robbery, respectively.

As demonstrated in Fig. 6, a crime clock is drawn in such a way that there are seven circles to represent the 7 days of a week on a Bristol board. A particular crime clock is declared only for one week. There are 24 divisions denoting 24 hours. It is almost impossible to use Bristol board crime maps for the analysis of past crimes generation and an automated crime clock map is desired.

Fig. 6. A manually drawn Crime Clock. The 24 divisions denote the 24 hours of a day. Seven parallel circles denote the seven days of a particular week. The two halves of the circle located in the center represent the crimes committed in the day time and the night time respectively. Circular annotations with the same set of colors which are used in the manual Crime Maps are used in locating the crime on the manual Crime Clock. For example, yellow color represents robbery.

SL-CIDSS Technical Framework

SL-CIDSS is designed and implemented as a distributed system which runs on the servers located at a central location of Sri Lanka Police and all the police stations are linked to the system through a VPN (virtual private network). SL-CIDSS is a platform independent system which is based on JAVA programming language. The layered architecture of SL-CIDSS provides a high scalability of new tools being installed so that the new functionalities can be added continuously. The property of extensibility is achieved by the incorporation of the independent semantic layers by extending Spring MVC [27]. As depicted in Fig. 7, SL-CIDSS is implemented using the Spring MVC (version – 4.1.5) framework [27]. AngularJS [25] was used in the view in order to have a MVC (Model- View- Controller) injection over the view. AngularJS is primarily used to provide reusability to html templates while generating AJAX request to change the model of each HTML view. Since SL-CIDSS core is written in Java programming language, any Java enabled web server can be used to run the system. Currently, Apache Tomcat 7.0 Web Server is used in running the system. Since SL-CIDSS is a web based system, a user can access any of the visualization tools, any report, any map or any CRUD (Create Read Update Delete) GUI, using an HTTP request. A particular tool corresponds to an ng-model [25] which is a directive in AngularJS and binds form elements to a property on the scope using ng-model Controller.

Fig. 7. The underlying architecture of SL-CIDSS. As SL-CIDSS is a distributed system, the users can send web requests to the system through one of the CRUD interfaces, analysis tools or reports. After loading a particular view, the data is passed through AJAX using the AngularJS API. The maps are rendered using OpenLayers API. Location based longitude/latitude information is converted to geographical information using the Point<->Geometry service and passed to the PostgreSQL database through the extended SpringMVC framework. REST API and the Jackson JSON Library is used to generate the JSON based AJAX responses. Hibernate has been used as the ORM storage. System.log file logs the system activities. PostgreSQL database acts as the primary database of SL-CIDSS.

ng-model Controller allows sending and receiving JSON data through HTTP requests and responses. Spring MVCRESTful [27] web services are used to invoke the SL-CIDSS analysis tools though http requests which were sent though ng-model controllers. Jackson JSON library [27] is used to convert the objects returned from the handlers to JSON format.

SL-CIDSS is composed of around 250 CRUD elements including the tools such as Crime map, Crime clock, Crime Hotspot tool, Pattern plotter, Modus operandi analysis and so on. Each of these elements communicates through JSON based GET/POST requests which makes SL-CIDSS a scalable system with independent control for each layer. For proper handling of transactions, the “Open Session in View” [28] pattern is used. It allows for lazy loading of associations in web views despite the original transactions already being completed.

Implementation Process

The system development was carried out in a version controlled environment. This was done using Netbeans 7.3.1 IDE [29] which supports revision controlled development by providing integrated tools. Bitbucket [30] was used as the repository provider for the hosting storage of the SL-CIDSS Git revision control. Bitbucket facilitates free private accounts up to 5 users [31]. The main reason for using Bitbucket was the availability of the interactive admin controlled system panel which facilitates online handling of project branches which is a concept that is frequently practiced in version controlled development to increase the code quality by letting an object under revision control to be modified parallely [32]. A third party Git client, SourceTree [33] was used to assist the version development process of SL-CIDSS. Whenever a new functionality is to be added to SL-CIDSS, a new branch was created and the new updates were added to the newly created branch. After confirming that the newly created content works fine with a code review, the branch that holds the new content is merged to the main branch. SL-CIDSS code backups were always maintained with the version control.

GIS Support of SL-CIDSS

One of the main features of the SL-CIDSS is GIS-based crime mapping. Fig. 8 depicts how SL-CIDSS facilitates GIS capabilities. Map layers are rendered through the OpenLayers Library [22]. The location based longitude/latitude information is converted to geographical data by using the “point to geometry” service implemented in between the OpenLayers WMS/WFS request and AngularJS request. This “point to geometry” service removes the necessity of using the external third-party web based geo service provider: Geoserver. When a user clicks on a map provided in SL-CIDSS, the “point to geometry” service will be activated and the generated geography data will be appended to the http request along with the other query data which is passed with the request. PostGIS extension of PostgreSQL database provides the capability in storing geographical data in the fields with the data type geography. This integration of GIS capabilities to SL-CIDSS allows the framework to visualize and analyse crime incidents with the help of geographical maps. In addition, with data mining methodologies such as geographical offender profiling, crime hotspot analysis, analysis of environmental factors that affect crimes using the geographical references, etc., the crime investigation process can be enhanced.

Fig. 8.GIS Module of SL-CIDSS. The geographical crime maps are rendered on a particular browser window using the OpenLayers API. The GIS Service generator which has been implemented as a service in the SL-CIDSS framework provides SL-CIDSS the capability of working with WFS/WMS services. PostgreSQL database with the PostGIS extension have made it possible for SL-CIDSS to store geographical information.

Enhanced Layered Functional Independency

Logic tier of SL-CIDSS is separated into more semantic layers to increase the functional independency as depicted in Fig. 9. In SL-SecureNet the logic layer is a pure inheritance of SpringMVC. However, in SL-CIDSS the logic layer is divided into 6 layers, namely: Service Controller Layer, Service Layer, Data Access Object (DAO) Controller Layer, DAO Layer, Extended ORM Layer, ORM Layer. The View Layer communicates with the Service Controller Layer in which all the controller classes are implemented in. All the logics related to the data mining tools and CRUD elements are implemented inside the Service Layer as Service implementation classes. The communication between the controllers and the service implementations is done through the service interfaces. The DAO (Data Access Object) Controller Layer is integrated to control the communication between the DAO Layer and the Service Layer. The data related implementations such as create, update read and delete are carried out in this layer. The lowermost layer is the Hibernate ORM Layer where the Object relational mapping storage is implemented. The Extended ORM inherits the ORM layer to add additional entity based capabilities. The DAO layer communicates with the Extended ORM Layer. This layered separation provides a very high functional independency in data, logic and view. This makes extension of SL-CIDSS less burdensome.

Fig. 9. Layered Architecture of SL-CIDSS Logic Model. Controller layer is composed of all the controller classes which communicates with the view and pass the information to the service

PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

layers. Service layer has all the logic implementation related to the data mining tools, reports and the CRUD elements. ORM layer is implemented with Hibernate. The layer of Hibernate entities communicates with the DAO Controller Layer through the DAO layer. Extended ORM Layer is composed of the abstract classes which extends the features of the ORM entities. DAO Layer provides a collection of concrete entities to be accessed by the Service layer through the DAO controller layer.

Data Model

One of the main features of SL-CIDSS is its data model that captures all aspects of crime recording and analysis. Data model consists of 64 entities covering all components of crime data recording and investigation. Also the data model is designed so that the data mining tools can access the data efficiently. The database is modelled in such a way that a data warehouse /data mart [34] can be easily converted to a fact constellation schema that centred on three facts: crime, suspect/accused and police officer.

User Interfaces and Data Retrieval

The graphical user interfaces and the visualization tools of SL-CIDSS are self-explanatory and users can be adapted to the system even without having an in-depth knowledge about computers. Web pages of SL-CIDSS are designed as tabbed document interfaces in which sets of related sections of the crime flow are grouped together. Moreover, our design approach makes sure that the web page sizes are very low since SL-CIDSS runs through AJAX based JSON http requests, the system can function even in low bandwidth networks. When a search query is executed in the system, it is subjected to many delays such as I/O delays and network communication delays. To overcome this , data indexing is incorporated in SL-CIDSS using Apache Lucene framework [35]. A search query of searching for a word in a collection of around 10 million tuples is reduced to an access time of 30 milliseconds by the introduction of Apache Lucene. It also allows rendering a result set of 250,000 tuples within an average of 50 seconds.

The user interfaces are categorized into 3 sections, namely Add/Edit/View Tab, Search Tab and Analysis/Reports Tab providing a tabbed interface which is depicted in Fig. 10 where the three buttons of the second bar provide the user the capability of loading a particular group of tabs categorized under a particular group. The tabs are colored in such a way that the sub groups of related entities are emphasized. Users are provided a composite view doing all the CRUD operations in one window as shown in Fig. 10 which provides the group of CRUD elements arranged in a tabbed interface. It provides the user a simplified outcome of the whole structure.

The navigation through the system screen and the menus are made easy by providing a sequence for the screens which goes along with the existing crime investigation system and the court processing system (See Fig. 4). When a user clicks on a particular tab, the view is loaded with the model using the AngularJS API. Therefore, the loading time of a particular tabbed view is minimal. The tabs are colored and grouped according to the similarities of the information hold. For example, the set of CRUD elements under the Crime Property entity, Crime Property Attributes entities and the Recovered Weapons entity are colored in pink as to give the user an idea that they can be grouped under one semantic.

Fig. 10. Tabbed interface view. The three buttons of the second bar provide the user the capability of loading a particular group of tabs categorized under a particular group. The tabs are colored in such a way that the sub groups of entities are emphasized.

Information Security and Backup

SL-CIDSS is incorporated with a security layer as shown in Fig. 7, which encrypts sensitive crime data using the Apache Shiro security framework [36]. Information such as name, age, address of a suspect or an accused is very sensitive information which should not be exposed to a third party. The passwords are encoded with bcrypt password hash algorithm which comes with Spring Security [37].

All the entities in the database are incorporated with the extra fields to store IP address of the machine, user ID, time and date of each transaction. The system validates authority value to a particular tuple so that the system determines whether a particular user has the read/write or just read authority to a particular record. Due to the precious value of the information in the means of law enforcement, when a user deletes a particular record, the status of that record will be changed to 'deleted' and it will not be displayed in the system, but, the record will not be removed from the database. The administrators can see the deleted content if a need arises. Fig. 11 shows the crime_record entity in which the aforementioned parameters are included. All the activities done in the system will be logged in textual format in an external file which is depicted in Fig. 7. SL-CIDSS provides an excellent backup service. A replicated database runs in a PostgreSQL server which runs in a separate server computer. An automated backup is generated from the database once per day and saved in two locations of Sri Lanka Police. The single account session count is limited to one so that no two users can login to the system using the same account information at the same time. Inactive sessions are invalidated after 5 minutes enforcing the user to login to the system again.

Fig. 11. crime_record database entity. insertip, insertuserid, inserttime, insertdate, updateip, updateuserid, updatetime, updatedate, and authority are the extra fields used for logging and auditing.

Role-Based Access Control Model of SL-CIDSS

Data access of SL-CIDSS is granted based on the police posts/ranks of Sri Lanka Police. Fig. 12 shows the area-wise data access privileges which are granted according to their police ranks or their designated posts. Director of CRD (Crime Record Division), IGP (Inspector General), and the chief Criminologist have the access to all island data. SDIG (Senior Deputy Inspector General of Police) of Range has the authority to access the resources related to his province. DIG (Deputy Inspector General of Police) and SSP (Senior Superintendent of Police) of District can access District resources, SSP and SP (Superintendent of Police) can access Division resources, and ASP (Assistant Superintendent of Police) can access Range (Three Police Stations) resources. OIC and other privileged police officers can access the station wise resources of SL-CIDSS.

Fig. 12. Police Post-wise system access privileges. Title of each vertical bar indicates a police post/s. The granularity of the area of legislation increases along the x-direction providing a decreased data accessibility. IGP, Director CRD and the Main Criminologist are the most privileged roles while the OIC or police officers are the least privileged roles.

The above mentioned data access privileges are implemented using a well-known security model named role-based access control model (RBACM) [38]**.** RBACM of SL-CIDSS is implemented with Spring Security, which focuses on providing both authentication and authorization to Java applications [39]. Data model for RBACM is depicted in Fig. 13 where a police officer has a RANK and a POST and works in a POLICE_STATION. A police station is located in a police DIVISION. A police division is located in a police DISTRICT. A district is located in a PROVINCE. A police officer has a user account. A police officer can have one or more roles in the system.

Fig. 13. Data model of the RBACM of SL-CIDSS. Figure shows the relationships among the database entities including police officer, rank, post, police_station, division, district, province, user account, role which facilitate the data storage for SL-CIDSS RBACM.

RBACM data model of SL-CIDSS was developed in such a way that the roles and the corresponding privileges can be assigned according to the current user level hierarchy shown in Fig. 12 which is developed using the administrative hierarchy of Sri Lanka Police. A particular police officer works in a particular police station which is located in a particular division. A district is composed of a collection of divisions and a province can have a collection of districts. ROLE entity is composed of six roles, namely SUPERUSER, PUSER, DISUSER, DIVUSER, RUSER, SUSER which are assigned with the data accessibilities according to the areas of legislations assigned as shown in Table 2.

Table 2.SL-CIDSS user roles and area of data access authorities

User Role	Data Availability
SUPERUSER	All island data
PUSER	Provincial data
DISUSER	District data
DIVUSER	Divisional data
RUSER	Regional data
SUSER	Station data

Police officer details are stored in the POLICE_OFFICER entity. A particular officer is then assigned with a particular role available in the ROLE entity and will be stored in the USER_ROLE entity. When a user logs into SL-CIDSS his/her role will be checked and the corresponding legislation of area will be stored in a session variable. Whenever he/she tries to access a particular record, the area of legislation will be checked against the authority field value and checked for his/her read/write permissions on the corresponding tuple.

Integrated Data Mining Tools

SL-CIDSS comes with a collection of crime data analysis tools. Crime clock tool, crime trend tool and the crime comparator tool are the general analysis tools which are used frequently in getting general information on the crime statistics. Crime clock tool provides the crime frequencies 24 hours a day for an area and time duration of preference. Crime comparator is implemented using a pie chart that provides a comparison of crime frequency percentages of selected crimes. Crime clock tool is implemented as a solution to the manual crime clock which is drawn on Bristol boards shown in Fig. 6. Crime trend tool provides a line chart comparison of the crime frequencies of different crime types for a given duration of time in a preferred area.

Drilldown analysis can be carried out using the advanced analysis tools which are integrated with SL-CIDSS. Crime hotspot tool, Modus Operandi analysis tool, Nearest police station detection tool, Crime association analysis tool, Deceptive record identification tool are considered as the advanced analysis tools which can be used to do drilldown analysis on crime data. Crime hotspot tool provides the hotspots available on a particular area of preference so that police can increase the security of that area to decrease the high crime magnitude. In Modus operandi analysis tool, a dynamic modus operandi (method of operation) is generated to a particular suspect using the crime patterns he/she has used in committing crimes. This dynamic modus operandi is then used in matching with a fuzzy based entropy value generated for the modus operandi of other crime scenes. In Nearest police station detection tool, J48 classification algorithm is trained to assign the geographical coordinates (longitudes and latitudes) to a set of predefined classes that are police stations distributed on the map of interest. This allows the system to assign an unknown coordinate point on a map to the nearest police station providing an option to the police officers to respond to an emergency situation very quickly. Association analysis tool can be used in two different ways. One way is to detect the deceptive records. It is a commonly known fact that suspects or accused might use different false identities and information at different situations. This hinders the process of capturing actual criminals due to difficulty in linking between crimes. To track such deceptive information, Deceptive record identification tool can be used. The tool runs a fuzzy text based search on the database to search for similar records. If the search finds a match with a similarity of over 60%, those records will be returned. Similarly the tool can be used to search the whole database under the user's preference to find out deceptive records. Crime association analysis tool can also be used to find associations between several crimes to find the related crimes committed in different areas of the country. Then the links can be used to capture the criminals. The Crime association analysis tool also works in the same way that deceptive record identification tool works. But, it conducts the fuzzy search on sub tuples with emphasize on groups of fields with similar semantics to be searched for similarity.

Results and Discussion

In this section, first a list of improvements of SL-CIDSS over SL-SecureNet is described in detail. This includes a performance comparison of the data retrieval process of SL-CIDSS and SL-SecureNet. This comparison was done using real crime data obtained from Sri Lanka Police. Finally software quality justification is presented including some user feedbacks of SL-CIDSS which are obtained from police officers around Sri Lanka.

Improvements of SL-CIDSS against SL-SecureNet

SL-SecureNet is basically designed for the aspect of crime mapping and analysis where the major emphasis is given to crime mapping. In SL-SecureNet, the geographical information is saved in a PostGIS database server. When the crime locations are to be annotated on the map, they were retrieved through the Geoserver [23] as vector layers on to the Google base map layers which were rendered by using OpenLayers [22]. The database is composed of only 9 entities in which 6 entities correspond to GCR (Grave Crime Record), Crime Place Address, Crime Type, Course Case, Police Station, Court Case Details and the other 3 entities are reserved for user role handling. The data available in the GCR entity is then used to generate outputs from the tools such as Crime locator, Crime clock, Periodic pattern visualizer, Crime map, Hotspot detection, Nearest police station detection, Crime comparator, Outbreak detection which are incorporated to the system. Following are the improvements of SL-CIDSS compared to SL-SecureNet.

1) Improved Graphical User Interface.

   SL-CIDSS graphical user interfaces are created by using HTML5 and CSS3. Bootstrap [40] is used in order to introduce responsive graphical user interfaces with user friendly GUI components which are not available in SL-SecureNet. With the introduction of responsive GUIs, one can use mobile devices to access the system in an interactive manner. The content viewing area is also enhanced with emphasizing the viewer's readability on current content. Tabbed interfaces are introduced to provide the information in a grouped manner as depicted in Fig. 10. SL-CIDSS also comes with a composite CRUD-MAP view which allows the user to do CRUD operations along with the in lined crime map as depicted in Fig. 14.

Fig. 14. A composite view in SL-CIDSS that includes a left sided map with a form used in inserting information. The map is used to locate a crime which is denoted by a red colored annotation. The form available in the right-hand side of the window is used to insert the information related to crime which is located on the map.

2) Introduction of a new data model incorporating 64 new entities to cover all aspects of crime data recording and to support effective analysis of crime data.

SL-SecureNet is composed of only 9 entities which mainly emphasize the fact of crime mapping and mapping related crime analysis. Almost all the tools which are available in SL-SecureNet use crime mapping information, while the others use the attribute data available in the GCR entity. But, the GCR system with crime investigation and crime analysis is much more complex and involves a huge amount of data recording as depicted in Fig. 4. SL-SecureNet provided a good platform to get user feedbacks in an easier manner. The feedbacks are then used towards analysing the domain thoroughly to identify the functional requirements along with data storage requirements. As a result of that, 64 entities were identified for the database of SL-CIDSS which will annihilate the problem of SL-SecureNet of not being able to work with other important data such as suspect information, court processing information, administrative data handling, system handling based on existing police post hierarchy and area of legislation, etc.

With the incorporation of these 64 entities, it became possible for more new functional requirements to be implemented, resulting in a CRUD entity count of around 250. As a result of newly incorporated entities, the new analysis tools and reports such as modus operandi analysis, association analysis, summary reports, annual progress reports, station progress reports, division progress comparisons and station progress comparison are implemented in addition to the tools available in SL-SecureNet.

3) Enhanced security with data encryption and enhanced user access.

User role handling on both SL-SecureNet and SL-CIDSS is done by inheriting Spring Security based user role handling. However, in SL-CIDSS, in addition to the extension of Spring Security, the content access is controlled using the regional and hierarchical police post legislative powers. The system always validates the user's level of accessibility depending on his/her police post. Then according to the post, the system decides the level of a real access to that particular user. This guarantees a high data security, while providing the users a customized view of the only crimes he/she has to work with. In SL-SecureNet passwords are encrypted with md5 hash algorithm. But in SL-CIDSS the passwords are encrypted with the BCrypt algorithm [37] which is claimed to be more secure than md5. Compared to the database of SL-SecureNet, the database of SL-CIDSS is composed of many entities where a very high level of security is necessary. Information, such as accused name, accused address, accused phone numbers and witness information are very sensitive. Therefore, an additional consideration is laid upon those data by adding an extra layer of encryption using the Apache Shiro security framework [36].

4) Hibernate object relational mapping (ORM) object storage and composite information searching facility

Hibernate 4.4.2 is used for object relational mapping in SL-CIDSS introducing more stability against the CRUD operations in the database. Due to the incorporation of Hibernate into SL-CIDSS, Hibernate Searching capability is added to SL-CIDSS. Although SL-SecureNet supports custom queries, the database is limited to have only simple searches. Also, since the system did not have indexing capabilities, searches consumed high amount of time. But, SL-CIDSS is incorporated with a searching facility which is implemented using the Hibernate Search framework [41] as SL-CIDSS is already incorporated with Hibernate [42]. Hibernate Search offers full-text search support for objects stored by Hibernate ORM. It allows searching words with text, ordering results by relevance and finding by approximation. The searching tool of SL-CIDSS provides a composite searching facility for users to search any content in a text based manner.

5) Exclusion of the additional web service “Geoserver”.

In order to save a crime location on the map in the PostgreSQL database, the longitude and latitude information of the crime scene has to be converted in to geography type under the correct geo reference system. In SL-SecureNet, this task is done by the Geoserver [23]. Geoserver then provides the capability to access a collection of geographical information through an http request using a web server (currently the jetty [43] web server is used by Geoserver).The process of displaying crimes in a map is slow since the request of retrieving geographical information is sent to Geoserver while crime related information is retrieved directly from the database server as shown in Fig. 15.

Fig. 15. SL-SecureNet information retrieval related to geographical and non-geographical data. When SL-SecureNet wants to render geographical information on the maps, the communication with the PostgreSQL database has to be done through the Geoserver. Non-geographical data can be retrieved by direct communication with the PostgreSQL database.

In SL-CIDSS, the necessity of Geoserver is removed by implementing a service which is triggered when user clicks on a particular map to add a crime record. When a user clicks on the map, the corresponding longitude and latitude information of that point is tracked and converted into a geography object and passed onto the database and saved as geographical data. This is because geographical data is supported by the PostgreSQL database server which is incorporated with the PostGIS extension which provides the PostgreSQL database server to support geographical information. When the geographical data is retrieved from the database to be displayed on the map, the geographical information is again converted into longitude and latitude data and displayed on the map. Therefore, the process of retrieving point information from the database becomes more efficient compared to the process of retrieving information through the Geoserver in SL-SecureNet.

6) Data sharing capabilities.

In crime analysis, it is very important to allow data sharing among other defence authorities. Spring MVC RESTful along with Jackson JSON library allows the SL-CIDSS framework to render AJAX based JSON responses as web services. This allows criminal justice information exchange between respective authorities within the country and outside the country. The web services are not accessible without an access key being validated, which should be passed with the web service URL. Any organization wanting to read the data provided in SL-CIDSS web services will have to provide read functions compliant to

JSON formats provided by SL-CIDSS. SL-CIDSS also accepts JSON web services which are compliant with SL-CIDSS JSON schemas.

7) Incorporation of AngularJS and Enhanced data retrieval capabilities using AJAX and Indexing.

The data retrieval process of SL-SecureNet is done using general GET and POST requests apart from the situational data and map view display rendered through the GeoEXT [44] API which provides GUI capabilities for OpenLayers map view and table views to be rendered together. AngularJS was incorporated to SL-CIDSS to make the process of data retrieval and HTML template usage for all CRUD operations for a particular function unique. The data binding and dependency injection eliminated much of the code and increased the system's code reusability. Data Indexing capability which is incorporated in SL-CIDSS using Apache Lucene framework [35] and AJAX request/response capability decreased the data retrieval time by keeping the page reloading down to a minimal.

8) Enhanced system auditing capabilities.

One of the very important functionalities of a system like SL-CIDSS should be its capability of software auditing. SL-CIDSS comes with software auditing tools whereas SL-SecureNet lacked software auditing. The tables of the database of SL-CIDSS are incorporated with columns such as insert_ip: to record the IP of the person who first inserted a particular record, insert_user_id: to record the user ID of the person who first inserted the record and so on. Also, SL-CIDSS maintains a text based log file which logs all the activities done on the system. These features ensure a good auditing capability in SL-CIDSS while maintaining a high level of security.

SL-CIDSS Performance Evaluation

To evaluate the performance of data retrieval step (i.e., data retrieval time) of the two versions, 4 tasks were performed, as shown in Table 3, and the results were compared. The experiment was carried out in a Windows server computer with 12 CPUs of Intel (R) Xeon (R) CPU of 2.4 GHz and a RAM of 8GB. Each query is provided with a task number from 1 to 4. Third column of Table 3 provides the information about the number of records returned by the queries. For the comparison, the retrieval of data from the GCR entity of SL-SecureNet and data from the crime_record entity in SL-CIDSS was considered. Also, all the queries were run in the localhost so that the data retrieval time is not subjected to network traffic. Table 4 shows the processing time taken by the two systems in running the four tasks provided in Table 3. SL-SecureNet is considered as System A and SL-CIDSS is considered as System B. Each task is run for 15 times and the results are displayed in milliseconds. Figs.16 - 19 show the boxplots of the time spent on each task by SL-SecureNet and SL-CIDSS. As depicted in Figs. 16 - 19, SL-CIDSS provides a good performance for data retrieval compared to SL-SecureNet as SL-CIDSS has taken less time for all the four tasks. Before any other statistical test was carried out, the normality of the data sets were tested using the Shapiro-Wilk test which is preferred to be one of the best normality tests for datasets with small sample sizes [45]. The normality test was carried out for the 8 datasets resulting under the four tasks by the two systems. The datasets 1A, 1B, 2A, 2B, 3A returned p-values less than 0.05 at the significance level of 5% proving that they are not normal. But the datasets 3B, 4A, 4B returned p-values greater than 0.05 at the significance level of 5% proving that those datasets are normal. Since, the test proved that the normality is not consistent, Kruskal-Wallis rank sum test was used for further analysis of the datasets. Kruskal-Wallis rank sum test [46] was conducted on all the datasets of time under the four tasks.

Table 3. Four tasks which are used to compare the efficiency of SL-CIDSS against SL-SecureNet.

Task No:	Task	Number of records returned
01	View the list of all the Robberies recorded in Kandy division from 01/01/2010 to 01/01/2015	742
02	View the list of all the crimes recorded in Kandy police division from 01/01/2010 to 01/01/2015	12385
03	View the list of all the Robberies recorded from 01/01/2010 to 01/01/2015	32605
04	View the list of all the crimes recorded from 01/01/2010 to 01/01/2015	277854

Table 4. Processing time of the two systems to run the four tasks provided in Table 1.

Task Number		**1**		**2**		**3**		**4**	
System		**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**
Processing time for each instance in milliseconds	**Iteration 1**	311	56	674	421	1913	1880	68324	51821
	Iteration 2	280	24	638	411	1918	1775	56747	50265
	Iteration 3	277	33	649	388	2157	1910	58618	50797
	Iteration 4	278	27	614	307	1936	1700	50544	40045
	Iteration 5	281	41	595	343	2312	1756	60124	58012
	Iteration 6	274	34	732	457	2047	1687	65214	50214
	Iteration 7	275	26	568	372	1912	1982	58247	45214
	Iteration 8	279	32	643	386	2004	1757	60542	58221
	Iteration 9	283	28	587	390	1905	2022	58012	48521
	Iteration 10	270	34	613	362	1963	1762	55212	52124
	Iteration 11	278	24	595	339	2006	1782	64725	60214
	Iteration 12	275	29	625	368	2318	1846	50012	52142

	Iteration 13	274	30	857	412	1995	1727	60325	58214
	Iteration 14	278	24	798	469	1906	1754	48215	48251
	Iteration 15	280	30	851	692	1921	1693	54214	48214

A denotes SL-SecureNet and B denotes SL-CIDSS.

Under all the four tasks Kruskal-Wallis rank sum test returned p-values less than 0.05 at the significance level of 5%, disproving the null hypothesis of amount of time spent have equal medians. Hence, the fact that SL-CIDSS performance is higher than the performance of SL-SecureNet which is shown in the boxplots of Figs. 16 - 19 is proved.

Fig. 16. Box plots for the processing time of System A and B for Task 1.

Fig. 17. Box plots for the processing time of System A and B for Task 2.

Fig. 18. Box plots for the processing time of System A and B for Task 3.

Fig. 19. Box plots for the processing time of System A and B for Task 4.

Software Quality Justification

Boehm, et. al. have divided the software quality into two categories: Current Usefulness and Potential Usefulness. The qualities which are expected from a software system in the user's point of view are categorized under current usefulness. The qualities which are expected from a software system in a developer's point of view are categorized under Current Usefulness. Under current usefulness the qualities such as efficiency, reliability, usability correctness, user friendliness and robustness are considered. Under Potential usefulness the qualities such as maintainability, modularity, reusability, and portability are considered [47]. SL-CIDSS is proven to not to be making wasteful use of system resources. Table 4 shows the query processing time of SL-CIDSS which shows a better efficiency compared to the earlier version SL-SecureNet. SL-CIDSS reliability is tested using the measurement of failure intensity which is the inverse of mean time to failure (MTTF) [48]. The average failure intensity of SL-CIDSS is 0.001 hr^{-1} and the failures which were resulted during the test phase were not fatal.

The system's target user group does not have much experience in ICT. Therefore, interactive help guidance throughout the system is provided to increase the usability of the system. The system's correctness was tested with code walkthrough, test cases and user reviews. The functionalities which did not adhere to its specified requirements were identified and fixed. The user friendliness of SL-CIDSS was increased by introducing new GUI elements using the technologies such as HTML5, CSS3, Bootstrap framework, etc. The version controlled development process of SL-CIDSS always provided a good maintainability, which supports the system to evolve to meet the changing needs. The version control method of development also helps the changes to be incorporated easily to satisfy new requirements or to correct deficiencies. The modularity was increased by introducing layers of codes depending on the aspect of use as shown in Fig. 9, which is an extension to the logic layer implemented using SpringMVC. This provides a higher modularity, and as a result it provides a very high reusability to the system components. As the system is developed using Java, the system can be used on any computer configuration other than its current one.

User Feedbacks

User feedback 1: The main issue solved with SL-CIDSS was the necessity of being physically present in the regional police stations to update the crime information. Now the police officers can update the system with day to day crime information directly from the respective police station.

User feedback 2: With the new system the police officers can maintain a profile in which they can view the information about the court cases they are involved in, and the things they have to carry for the next court date. Police officers can maintain the information on the supervision of the accused.

User feedback 3: One of the main problems available in the manual system was the problem of determination whether the suspects have been previously convicted for crimes. Another problem is the unavailability of the criminal information which is older than 5 years. Also the lack of searching capability in searching the huge stacks of files to check the availability of information on criminals in the past records is a big issue. With these constraints the other problem is the result of deceptive records. Since, there is no validation procedure, the suspects happen to provide false information. But, the introduction of SL-CIDSS, has provided the capability of searching the database for previous convictions and at the same time providing the capability of checking the information of a particular criminal to be deceptive or not.

User feedback 4: One of the main advantages of SL-CIDSS is the capability to retrieve information within a very short time, which was less than 5 seconds for most cases. The analysis tools of SL-CIDSS give a great help in generating timely decisions. Tools such as hotspot detection tool provide enough information in utilizing police petrol services in different location in a logical manner.

User feedback 5: Everything related to GCR can be viewed compositely from one system. Normally the records related to accused are maintained from one place, information about court cases is maintained at one place, information about GCR records is maintained at another place, crime locations are annotated on Bristol boards, crime clocks are drawn on Bristol boards. Seeing a composite view which relates GCR to accuse and to view geographical information related to GCR is not available in the manual system. Now all of these problems are resolved with one system which provides a relational view of all this information.

Conclusion

A novel data mining framework which tallies the GCR crime maintenance structure was introduced. The decision support tools of the system have directly influenced the crime solving rate due to its fast data retrieval capability which was utilized with data indexing and AJAX. Now with SL-CIDSS, the process of crime reporting can be done at main regional police stations automatically through the system. It eliminates the need of preparing paper based summary reports manually by spending long hours and handing them physically to respective regional police stations. The centralized database of SL-CIDSS has made crime data available to all the police stations and related institutions in Sri Lanka, providing a very fast access to the data related to any crime related situation at hand. The improved graphical user interfaces and the guided help increased the usability of the system. The improved AJAX capabilities and the Indexing power of the of SL-CIDSS has increased the efficiency compared to its old version SL-SecureNet.The framework utilizes an open space for more data mining tools such as entity mining, image processing techniques to be incorporated in an easy manner without having to worry about the internal architecture in the future. The enhanced security of SL-CIDSS provides a trustable repository of data not being subjected to eavesdropping. The data sharing capabilities of SL-CIDSS were enhanced with web services so that the respective authorizes can work with SL-CIDSS in an interoperable manner.

Acknowledgments

We would like to acknowledge Sri Lanka Police for the support they provided to make the project a success.

References

1. Information Technology Division of Sri Lanka Police. Sri Lanka Police. [Internet].; 1998 [cited 2015 03 22]. Available: http://www.police.lk/index.php/component/content/article/190.
2. Library T'L. The 'Lectric Law Library. [Internet]. [cited 2015 06 05]. Available: http://www.lectlaw.com/files/int20.htm.
3. Lederman D, Fajnzylber NLP." What causes violent crime?". European Economic Review. 2002; 46: p. 1323-1357.
4. Chen H, Chung W, Xu JJ, Wang G, Qin Y, Chau M. Crime Data Mining: A general framework and some examples. Computer. 2014 April; 37(0018-9162): p. 50-56.
5. Mauro M. Psycholgy Today. [Internet].; 2010 [cited 2015 04 04]. Available: https://www.psychologytoday.com/blog/take-all-prisoners/201003/catch-serial-criminal.
6. Frey BJ , Dueck D. Clustering by Passing Messages Between Data Points. SCIENCE. 2007 Feb 16; 315: p. 972-976.

7. PostgreSQL Global Development Group. PostgreSQL. [Internet].; 1996 [cited 2012 05 07]. Available: http://www.postgresql.org/.
8. Chen H, Schroeder J, Hauck RV, Ridgeway L, Atabakhsh H, Gupta H, Boarman C, Rasmussen K, Clements AW. COPLINK Connect: Information and knowledge management for law enforcement. Decision Support Systems. 2002;(34): p. 271-285.
9. United States Department of Justice. Uniform Crime Reporting: National Incident-Based Reporting System, Data Collection Guidelines; 1998.
10. Crime Reports. [Internet].; 2009 [cited 2015 01 22]. Available: https://www.crimereports.com/.
11. Calhoun CC, Stobbart CE, Thomas DB, Villarrubia JA, Brown DE. Improving Crime Data Sharing and Analysis Tools for a Web-Based Crime Analysis Toolkit: WebCAT 2.2. In Proceedings of the 2008 IEEE Systems and Information,Engineering Design Symposium, University of Virginia; 2008; Charlottesville: IEEE. p. 40-45.
12. Oatley B, Ewwart B. Data mining and crime analysis. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2011; 1(2): p. 147-153.
13. About COPLINK project. [Internet].; 2011 [cited 2011 07 12]. Available: http://ai.bpa.arizona.edu/research/coplink/.
14. Rhodes CJ, Keefe EMJ. Social Network Topology: A Bayesian Approach. The Journal of Operational Research Society. 2007 Dec; 58(12): p. 1605-1611.
15. Offender Profiling. [Internet].; 2011 [cited 2011 11 2]. Available: http://www.liv.ac.uk/psychology/ccir/op.html.
16. Gupta GK. Introduction to Data Mining with Case Studies. 3rd ed. Delhi: PHI Learning Pvt. Ltd.; 2014.
17. Imielinkski T, Swami A, Agrawal R. Mining Association rule between sets of items in large databases. In Proceedings of the ACM SIGMOD International Conference of Management of Data; 1993; New York: Association for computer machinery. p. 207-216.
18. Han J, Koperski K. Discovery of spatial association rules in geographic information databases. In Proceeding of the 4th International Symposium on Spatial Databases; 1995: Advances in Spatial Databases. p. 47-67.
19. Chen H. Intelligence and security informatics for international security. 1st ed.: Springer US; 2006.
20. Chen H. Machine learning for information retrieval: neural. Journal of the American Society for Information Science. 1995; 46(3): p. 194-216.
21. Chamikara MAP, Yapa YPRD, Kodituwakku SR, Gunathilake J. SL-SecureNet: Intelligent Policing Using Data Mining Techniques. International Journal of Soft Computing and Engineering (IJSCE). 2012 Mar; 2(1): p. 175-180.
22. OpenLayers Dev Team. OpenLayers. [Internet].; 2006 [cited 2012 02 24]. Available: http://openlayers.org/.
23. Open Source Geospatial Foundation. Geoserver. [Internet].; 2010 [cited 2012 02 03]. Available: http://geoserver.org/.
24. Shekhar S, Xiong H. Encyclopedia of GIS. 2008th ed. New York: Springer; 2007.

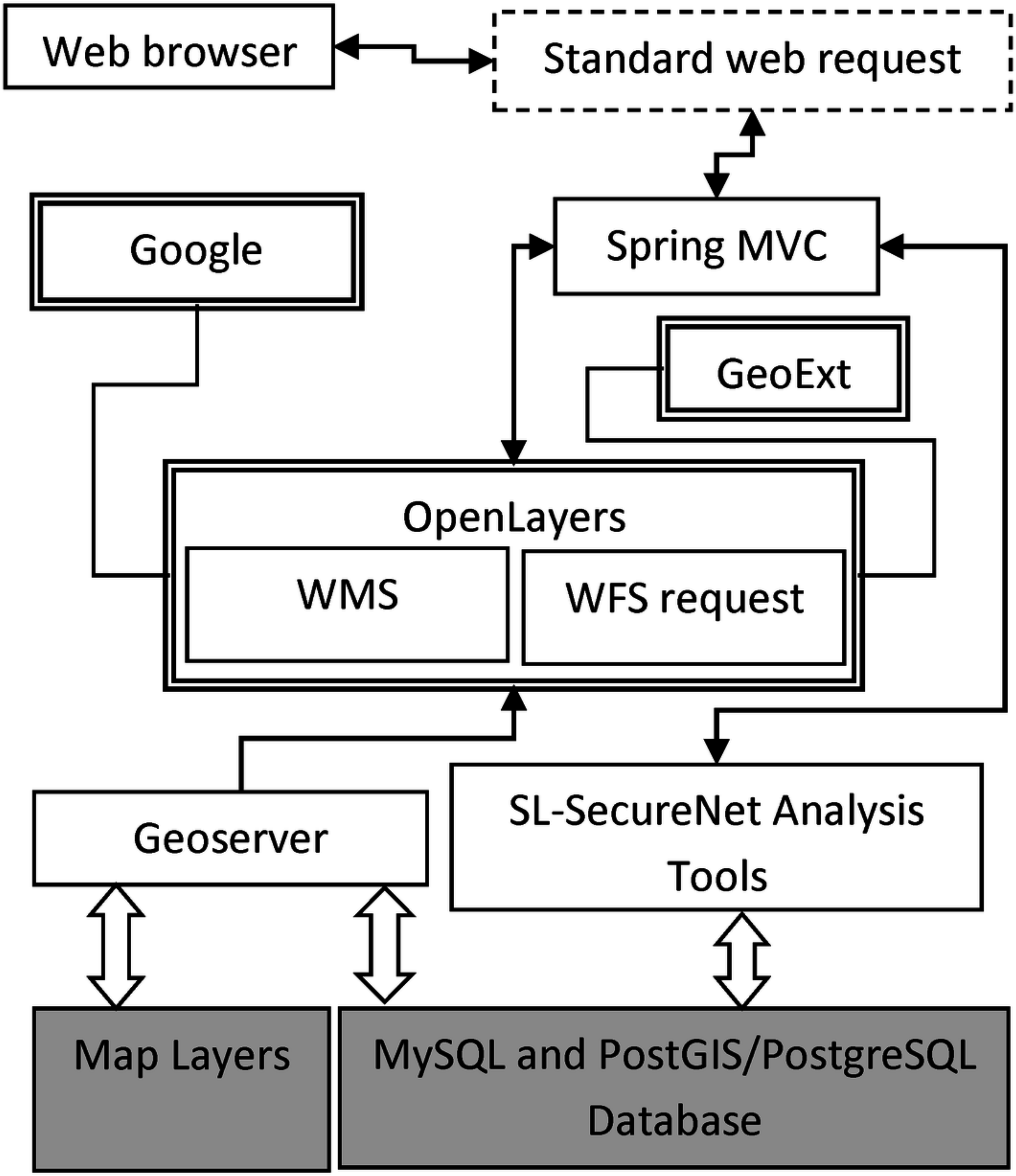
25. Green B, Seshadri S. AngularJS. 1st ed.: O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.; 2013.
26. Pressman RS. Software Engineering-A Practitioner's Approach. 7th ed.: McGraw-Hill; 2010.
27. Walls C. Spring in Action. 3rd ed.: Manning Publications; 2011.
28. Pivotal Software. Spring. [Internet].; 2014 [cited 2014 11 10]. Available: http://docs.spring.io/spring-framework/docs/3.2.13.RELEASE/javadoc-api/org/springframework/orm/hibernate3/support/OpenSessionInViewInterceptor.html.
29. Oracle. NetBeans. [Internet].; 2013 [cited 2015 02 24]. Available: https://netbeans.org/community/releases/73/.
30. Atlassian. Bitbucket. [Internet].; 2011 [cited 2013 10 03]. Available: https://bitbucket.org/.
31. Loeliger J, McCullough M. Version Control with Git. 2nd ed.: O'Reilly; 2012.
32. Vogel L. Working with branches. In Vogel L. Distributed Version Control with Git: Mastering the Git command line. 2nd ed.; 2013. p. 71-73.
33. Atlassian. SourceTree. [Internet].; 2014 [cited 2014 10 11]. Available: https://www.sourcetreeapp.com/.
34. Prabhu CSR. Data Marts. Prabhu CSR. Data Warehousing. 3rd ed. New Delhi: PHI Learning Private Limited; 2008. p. 1-7.
35. The Apache Software Foundation. The Apache Software Foundation. [Internet].; 2012 [cited 2014 05 06]. Available: https://lucene.apache.org/.
36. The Apache Software Foundation. The Apache Software Foundation. [Internet].; 2008 [cited 2014 12 01]. Available: http://shiro.apache.org/.
37. Pivotal Software. Spring. [Internet].; 2015 [cited 2015 03 20]. Available: http://docs.spring.io/autorepo/docs/spring-security/3.2.4.RELEASE/apidocs/org/springframework/security/crypto/bcrypt/BCrypt.html.
38. Ferraiolo DF, Kuhn DR. Role-based Access Control. 2nd ed. Norwood: Artech house, INC.; 2003.
39. Pivotal Software. Spring. [Internet].; 2013 [cited 2013]. Available: http://projects.spring.io/spring-security/.
40. Otto M, Thornton J. Bootstrap. [Internet].; 2011 [cited 2012 03 04]. Available: http://getbootstrap.com/.
41. JBossDeveloper redhat. Hibernate. [Internet].; 2008 [cited 2014 04 05]. Available: http://hibernate.org/search/.
42. Red Hat. Hibernate. [Internet].; 2015 [cited 2015 04 04]. Available: http://hibernate.org/.
43. The Eclipse Foundation. eclipse. [Internet].; 2009 [cited 2015 01 24]. Available: http://eclipse.org/jetty/.

44. GeoExt Community. GeoExt. [Internet].; 2009 [cited 2010 09 15]. Available: http://geoext.org/.
45. Sen A, Srivastava M. Regression Analysis. 1st ed.: Springer; 1990.
46. Longnecker M, Ott RL. An Introduction to Statistical Methods and Data Analysis. 6th ed.: Macmillan Publishing Solutions; 2010.
47. Boehm BW, Brown JR, Lipow M. Quantitative Evaluation of Software Quality. In Proceedings of 2nd IEEE International Conference on Software Engineering; 1976; California. p. 592-605.
48. Malaiya YK. Software Reliability and Security. Encyclopedia of Library and Information Science. 2005;: p. 1-12.

1

Fig. 1 . Architecture of SL-SecureNet

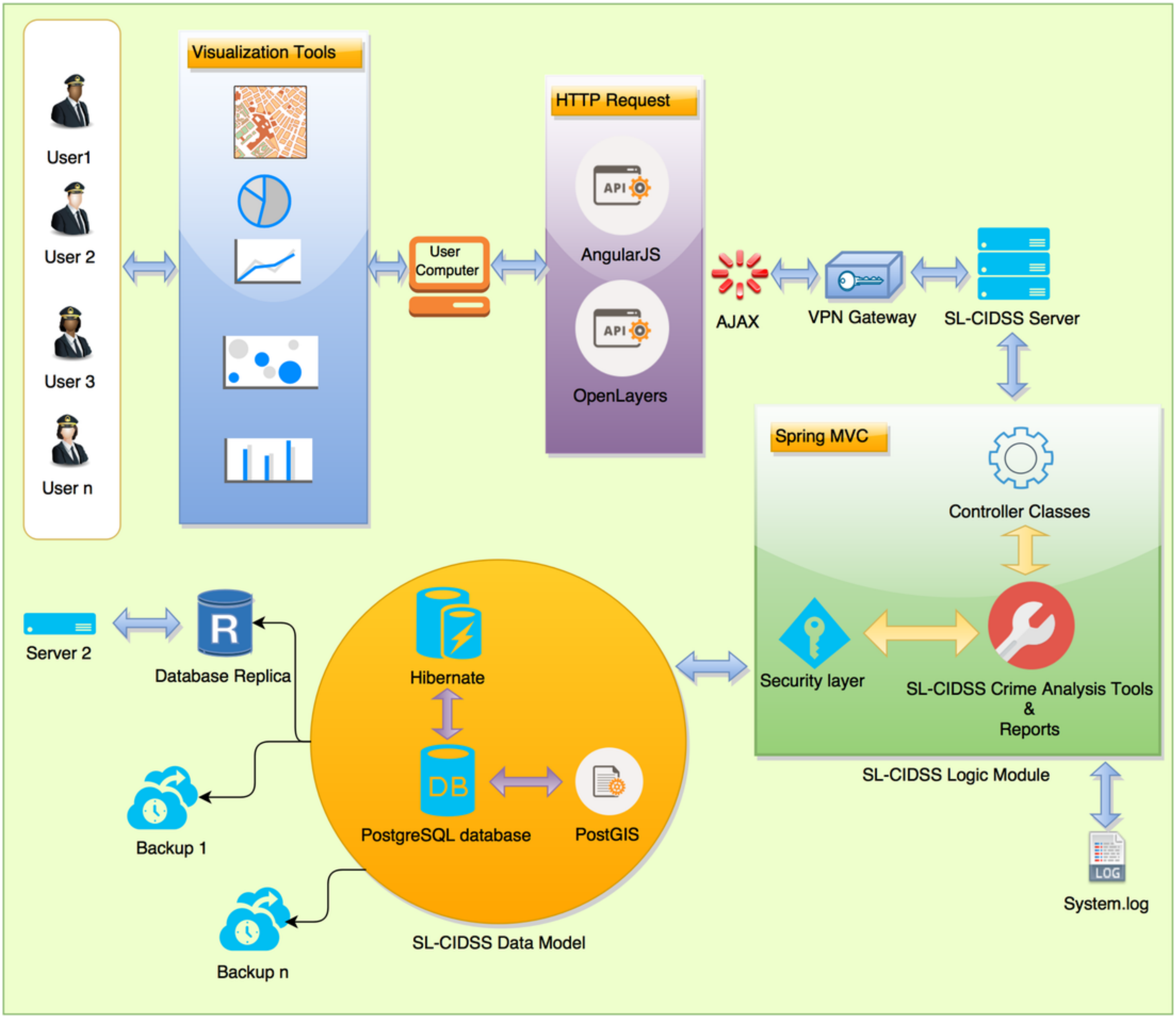
Architecture of SL-SecureNet. The controllers implemented in the Spring MVC framework direct the standard user requests to the corresponding logic. OpenLayers API is used in rendering the maps. Geoserver works as the middleware which facilitates WFS and WMS services in generating the map layers. The PostgreSQL database works as the primary data storage of SL-SecureNet. A MySQL database is used to store the data of the integrated data mining tools.


Web browser
Standard web request
Google
Spring MVC
GeoExt
OpenLayers
WMS
WFS request
Geoserver
SL-SecureNet Analysis Tools
Map Layers
MySQL and PostGIS/PostgreSQL Database

2

Fig. 2. Main elements and their interactions of SL-CIDSS

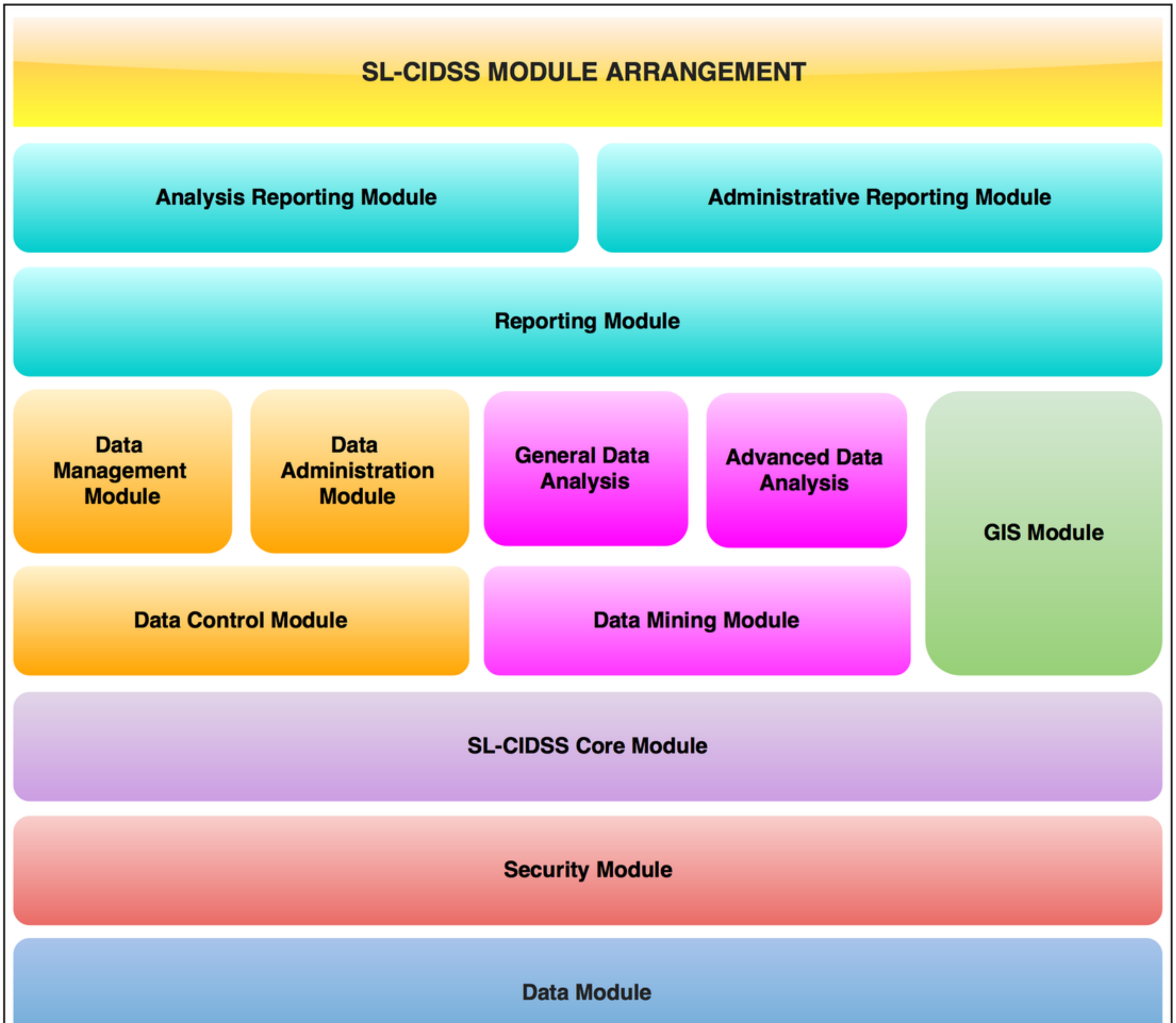
Police officers from any police station can access the tools which are facilitated by SL-CIDSS through the VPN. AngularJS and OpenLayers APIs are used in generating a tool related or a map related AJAX request. The system is accessible only through a VPN. SL-CIDSS runs in a web server installed in a server computer located in the Police Headquarters. SpringMVC works as the base framework for SL-CIDSS. SL-CIDSS data model includes the PostgreSQL database with GIS capabilities enabled using the PostGIS extension. System.log is an external file which logs all the system activities in textual format. The database is replicated and the backups are generated once per day.


User1
User 2
User 3
User n
Visualization Tools
User Computer
HTTP Request
AngularJS
OpenLayers
AJAX
VPN Gateway
SL-CIDSS Server
Spring MVC
Controller Classes
Security layer
SL-CIDSS Crime Analysis Tools
&
Reports
SL-CIDSS Logic Module
System.log
Server 2
Database Replica
Hibernate
PostgreSQL database
PostGIS
Backup 1
Backup n
SL-CIDSS Data Model

3

Fig. 3. Main module arrangement of SL-CIDSS

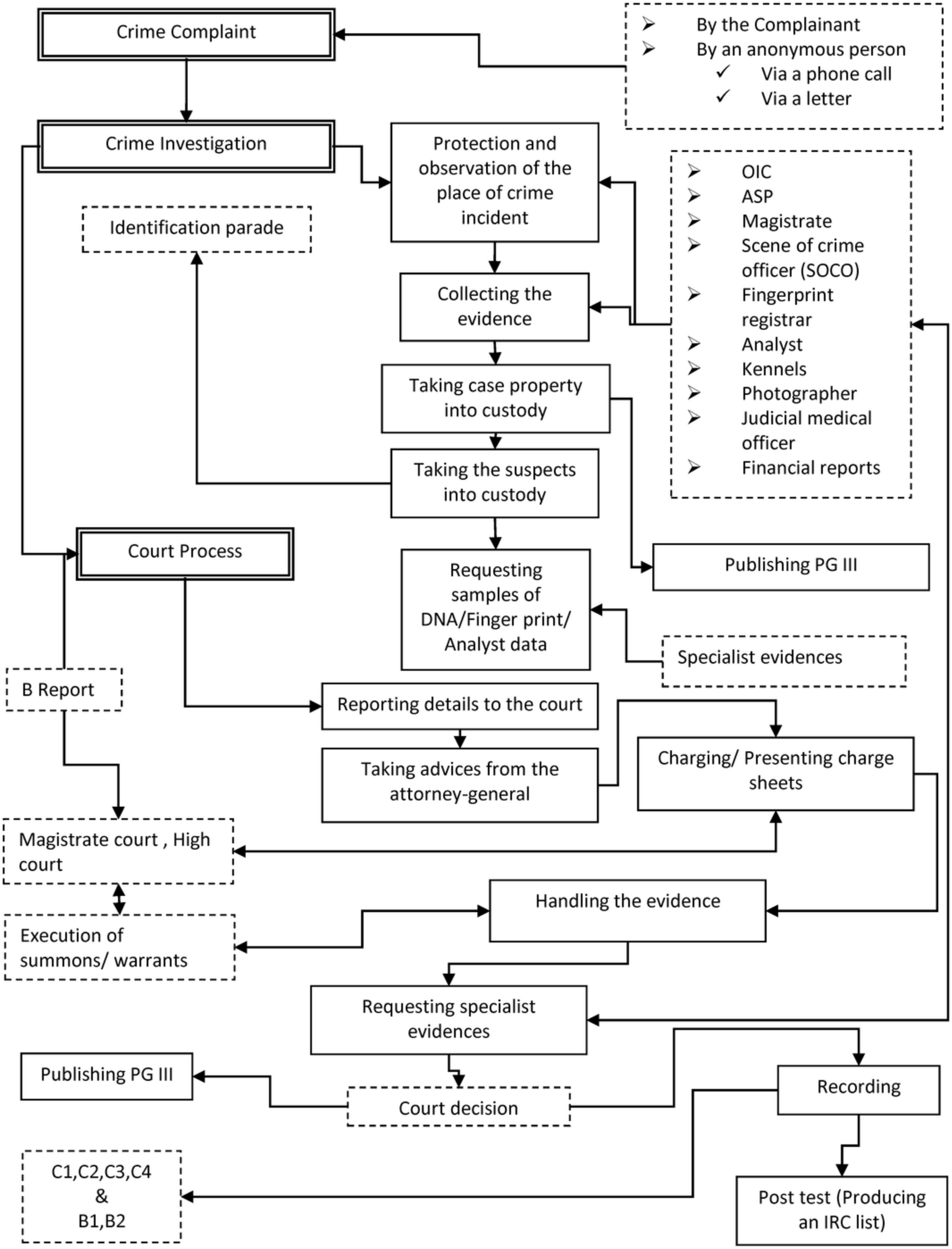
SL-CIDSS functionalities/services are divided in to modules and related modules are grouped. Each module group is colored using the same color. For example Data Control Module, Data Management Module and Data Administration Module are colored with orange color because the Data Control Module comes as two modules namely Data Management Module and Data Administration Module.



4

Fig. 4. Flow of events in the Manual crime recording and investigation and court processing system.

Double lined elements are the major entities. Single lined entities are the activities carried out under each major entity and the entities with dashed lines represent transient objects which are corresponding to either an input or an output instance.


Crime Complaint
By the Complainant
By an anonymous person
Via a phone call
Via a letter
Crime Investigation
Protection and observation of the place of crime incident
Identification parade
OIC
ASP
Magistrate
Scene of crime officer (SOCO)
Fingerprint registrar
Analyst
Kennels
Photographer
Judicial medical officer
Financial reports
Collecting the evidence
Taking case property into custody
Taking the suspects into custody
Court Process
Publishing PG III
Requesting samples of DNA/Finger print/ Analyst data
Specialist evidences
B Report
Reporting details to the court
Taking advices from the attorney-general
Charging/ Presenting charge sheets
Magistrate court , High court
Execution of summons/ warrants
Handling the evidence
Requesting specialist evidences
Publishing PG III
Court decision
Recording
C1,C2,C3,C4
&
B1,B2
Post test (Producing an IRC list)

5

Fig. 5. A manually drawn crime map

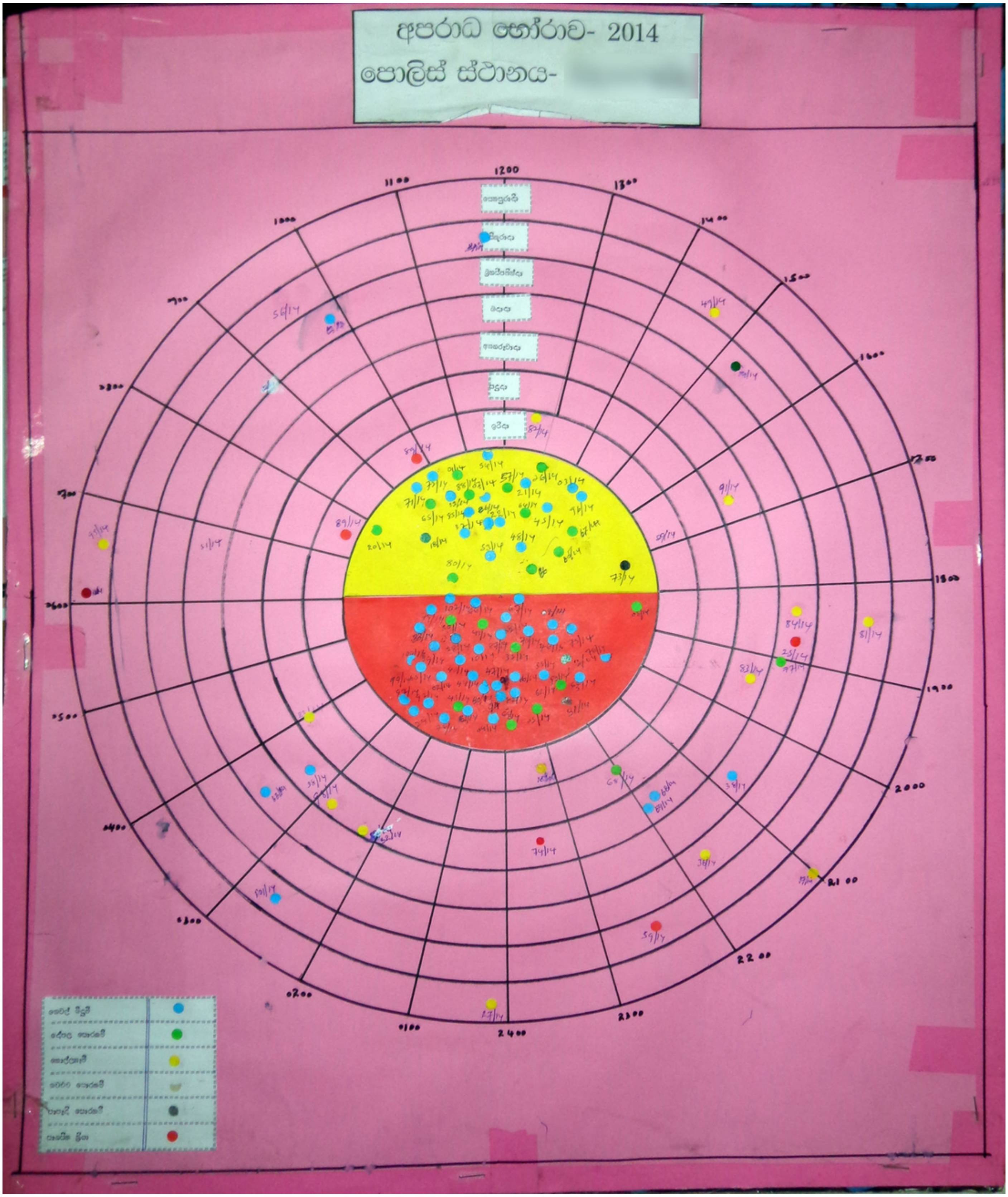
A map corresponds to a particular area of jurisdiction. Colored circular annotations represent different crime types. For instance, red , blue, black and yellow are used to denote homicide, burglary, theft, and robbery, respectively.

PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

6

Fig. 6. A manually drawn Crime Clock

The 24 divisions denote the 24 hours of a day. Seven parallel circles denote the seven days of a particular week. The two halves of the circle located in the center represent the crimes committed in the day time and the night time. Circular annotations with the same set of colors which are used in the manual Crime Maps are used in locating the crime on the manual Crime Clock. For example, yellow color represents robbery.



PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

7

Fig. 7. The underlying architecture of SL-CIDSS

As SL-CIDSS is a distributed system, the users can send web requests to the system to one of the CRUD interfaces, analysis tools or reports. After loading a particular view, the data is passed through AJAX using the AngularJS API. The maps are rendered the using OpenLayers API. Location based longitude/latitude information is converted to geographical information using the Point<->Geometry service and passed to the PostgreSQL database through the extended SpringMVC framework. REST API and the Jackson JSON Library is used to generate the JSON based AJAX responses. Hibernate has been used as the ORM storage. System.log file logs the system activities. PostgreSQL database acts as the primary database of SL-CIDSS.

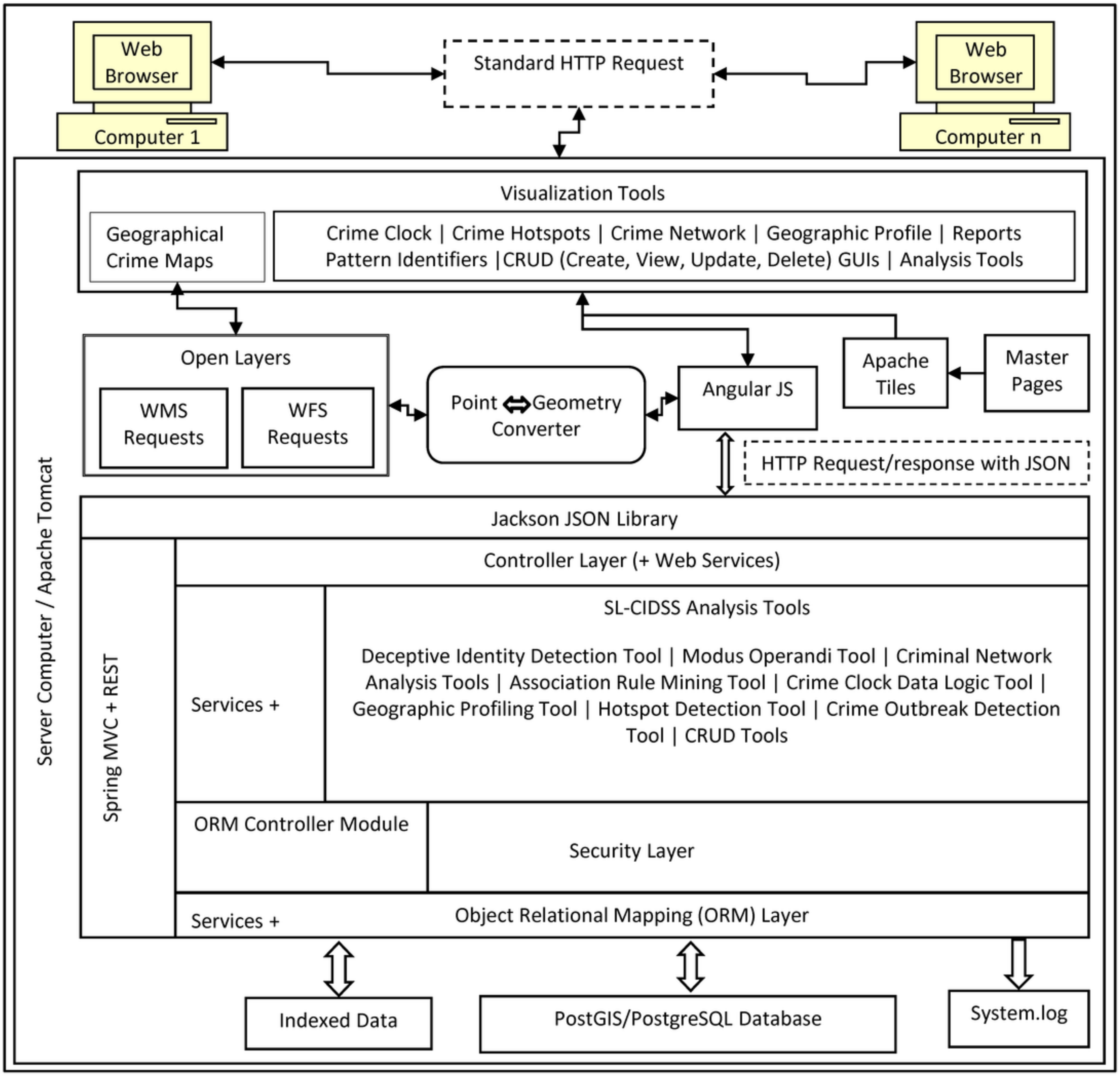
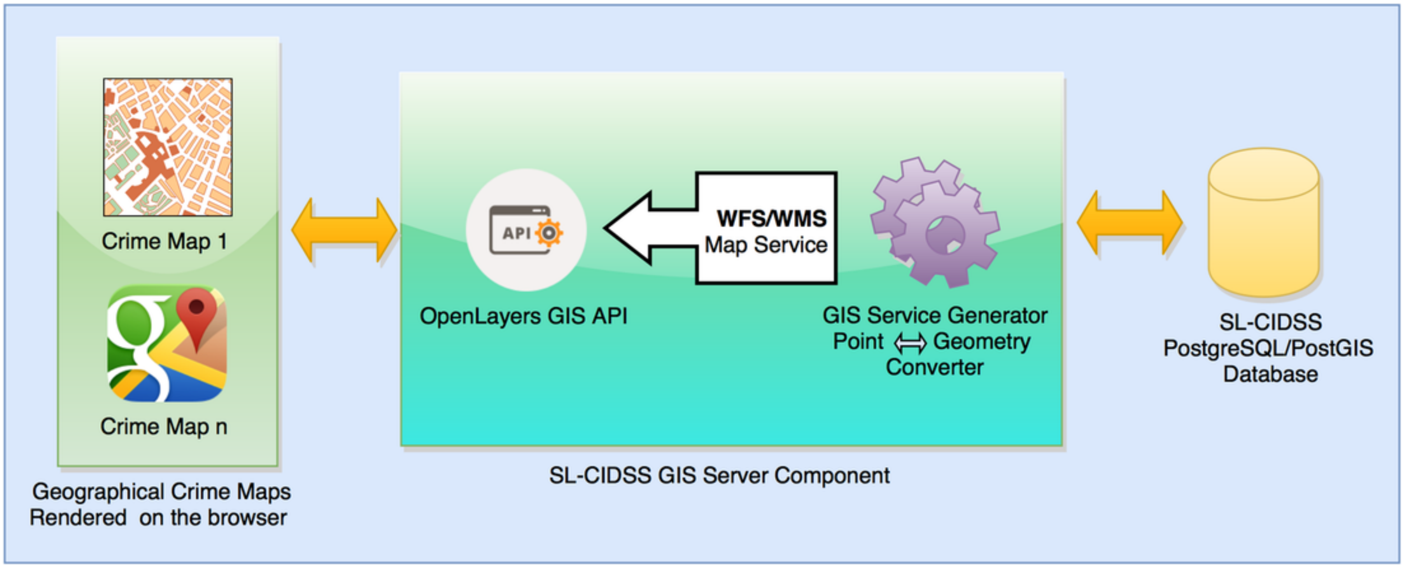

Web Browser
Computer 1
Standard HTTP Request
Web Browser
Computer n
Visualization Tools
Geographical Crime Maps
Crime Clock | Crime Hotspots | Crime Network | Geographic Profile | Reports
Pattern Identifiers |CRUD (Create, View, Update, Delete) GUIs | Analysis Tools
Open Layers
WMS Requests
WFS Requests
Point ⇔ Geometry Converter
Angular JS
Apache Tiles
Master Pages
HTTP Request/response with JSON
Server Computer / Apache Tomcat
Jackson JSON Library
Spring MVC + REST
Controller Layer (+ Web Services)
Services +
SL-CIDSS Analysis Tools
Deceptive Identity Detection Tool | Modus Operandi Tool | Criminal Network Analysis Tools | Association Rule Mining Tool | Crime Clock Data Logic Tool | Geographic Profiling Tool | Hotspot Detection Tool | Crime Outbreak Detection Tool | CRUD Tools
ORM Controller Module
Security Layer
Services +
Object Relational Mapping (ORM) Layer
Indexed Data
PostGIS/PostgreSQL Database
System.log

Fig. 8.GIS Module of SL-CIDSS

The geographical crime maps are rendered on a particular browser window using the OpenLayers API. The GIS Service generator which has been implemented as a service in the SL-CIDSS framework provides SL-CIDSS the capability of working with WFS/WMS services. PostgreSQL database with the PostGIS extension have made it possible for SL-CIDSS to store geographical information.

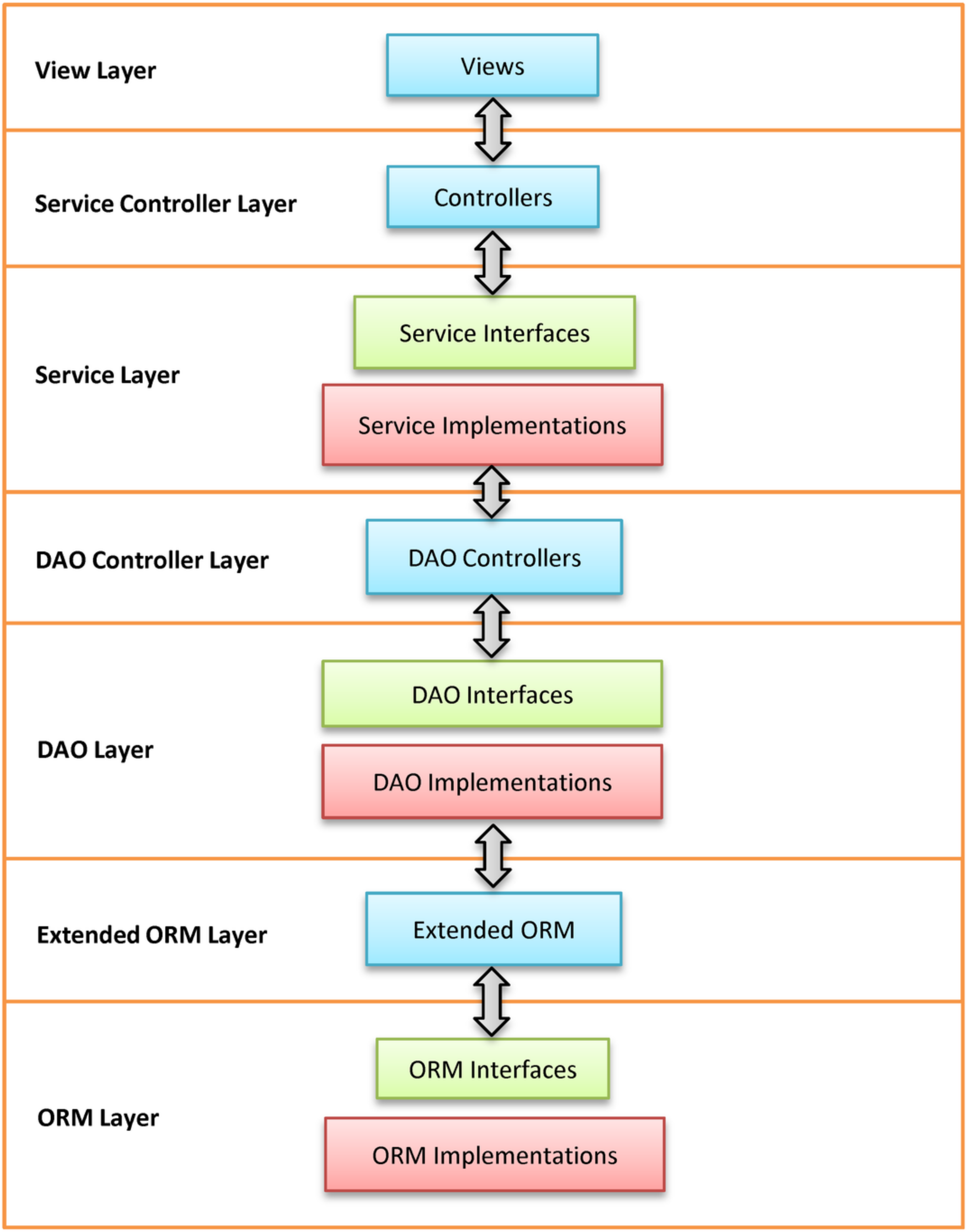


PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

9

Fig. 9. Layered Architecture of SL-CIDSS Logic Model

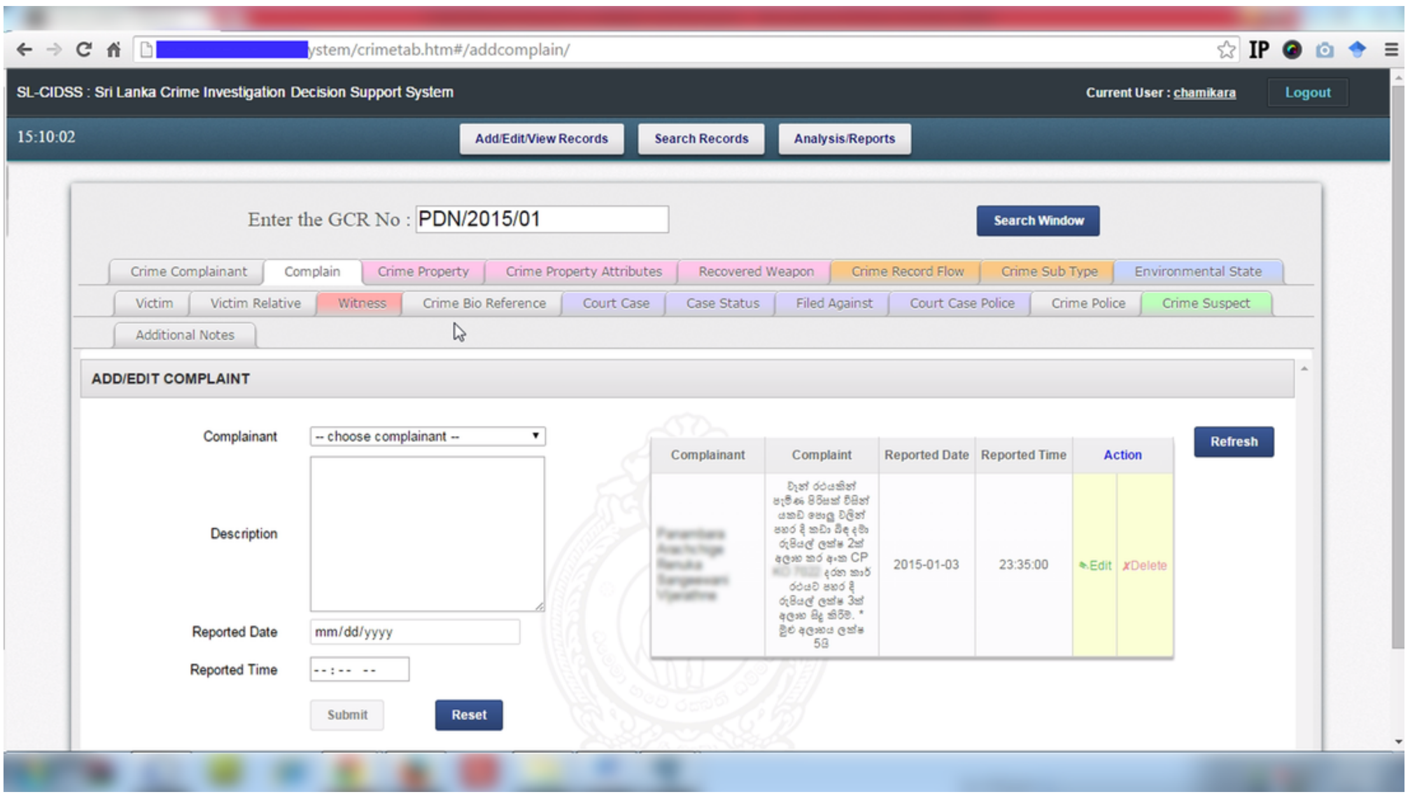
Controller layer is composed of all the controller classes which communicate with the view and pass the information to the service layers. Service layer has all the logic implementation related to the data mining tools, reports and the CRUD elements. ORM layer is implemented with Hibernate. The layer of Hibernate entities communicates with the DAO Controller Layer through the DAO layer. Extended ORM Layer is composed of the abstract classes which extends the features of the ORM entities. DAO Layer provides a collection of concrete entities to be accessed by the Service layer through the DAO controller layer.


View Layer
Views
Service Controller Layer
Controllers
Service Layer
Service Interfaces
Service Implementations
DAO Controller Layer
DAO Controllers
DAO Layer
DAO Interfaces
DAO Implementations
Extended ORM Layer
Extended ORM
ORM Layer
ORM Interfaces
ORM Implementations

10

Fig. 10. Tabbed interface view

The three buttons of the second bar provide the user the capability of loading a particular group of tabs categorized under a particular group. The tabs are colored in such a way that the sub groups of entities are emphasized.



11

Fig. 11. crime_record database entity

insertip, insertuserid, inserttime, insertdate, updateip, updateuserid, updatetime, updatedate, and authority are the extra fields used for logging and auditing.

crime_record

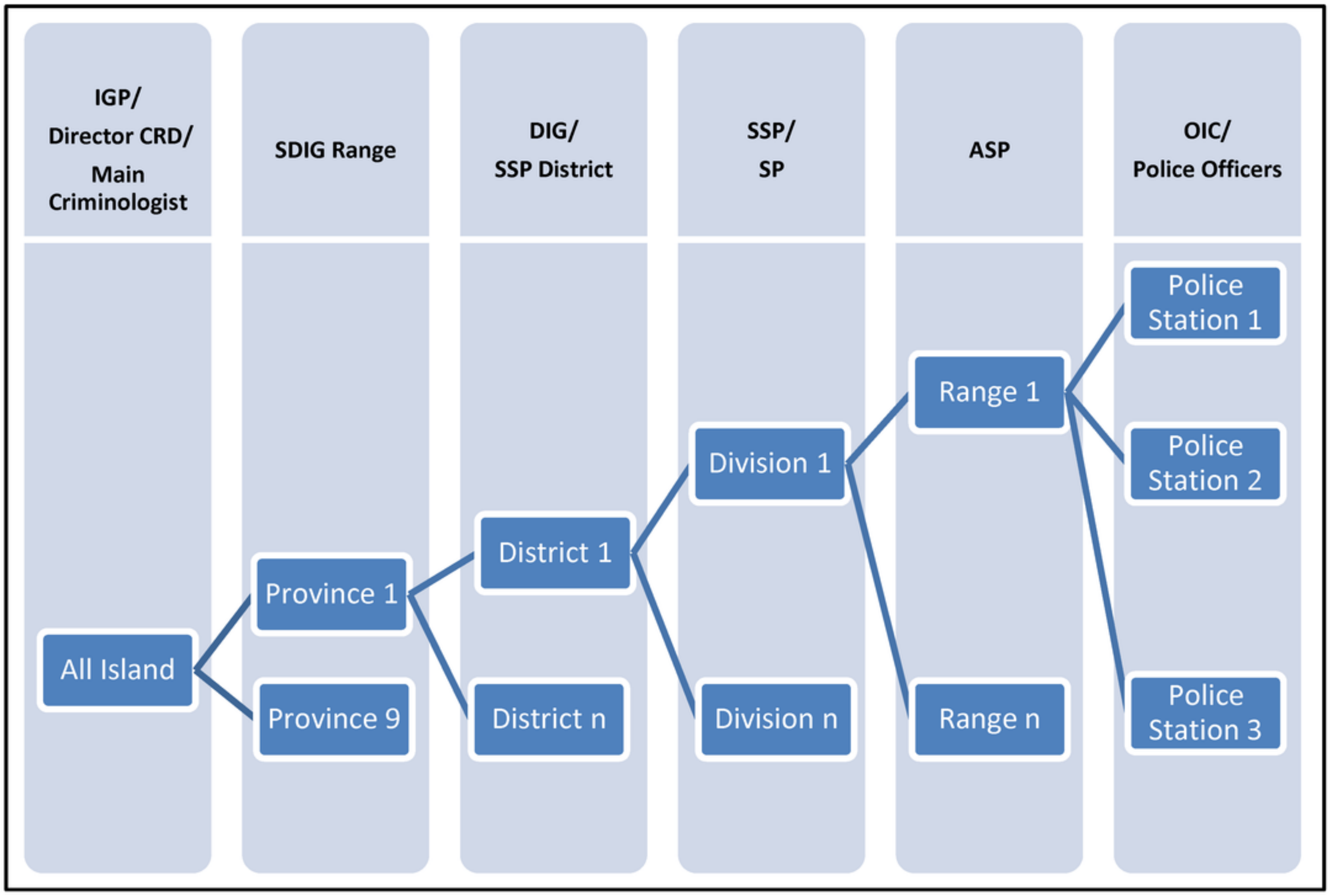
gcrno	INTEGER
crime_address_cano	INTEGER
crime_type_ctno	INTEGER
court_case_caseno	INTEGER
police_station_stno	INTEGER
ibreferenceno	INTEGER
crimelocaddress	CHARACTER VARYING(70)
dateofcrime	DATE
timeofcrime	TIME(6) WITHOUT TIME ZONE
the_geom	USER-DEFINED
insertip	CHARACTER VARYING
insertuserid	INTEGER
updateuserid	INTEGER
insertdate	DATE
updatedate	DATE
updateip	CHARACTER VARYING
authority	INTEGER
inserttime	TIME(6) WITHOUT TIME ZONE
updatetime	TIME(6) WITHOUT TIME ZONE
drepnum	CHARACTER VARYING
sdateofcrime	CHARACTER VARYING(255)
stimeofcrime	CHARACTER VARYING(255)
isvalidate	BOOLEAN
crdreference	CHARACTER VARYING(255)
realgcr	CHARACTER VARYING(255)

PeerJ PrePrints | https://dx.doi.org/10.7287/peerj.preprints.1529v1 | CC-BY 4.0 Open Access | rec: 24 Nov 2015, publ: 24 Nov 2015

12

Fig. 12. Police Post-wise system access privileges

Title of each vertical bar indicates a police post/s. The granularity of the area of legislation increases along the x-direction providing a decreased data accessibility. IGP, Director CRD and the Main Criminologist are the most privileged roles while the OIC or police officers are the least privileged roles.



13

Fig. 13. Data model of the RBACM of SL-CIDSS

The figure shows the relationships among the database entities including police officer, rank, post, police_station, division, district, province, user account, role which facilitate the data storage for SL-CIDSS RBACM.

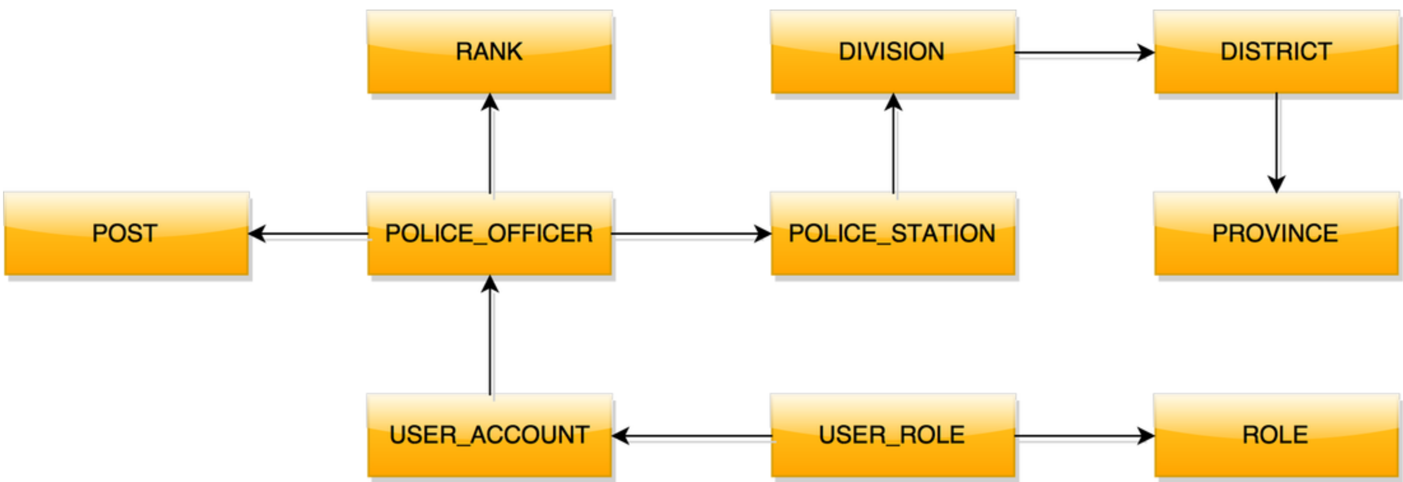
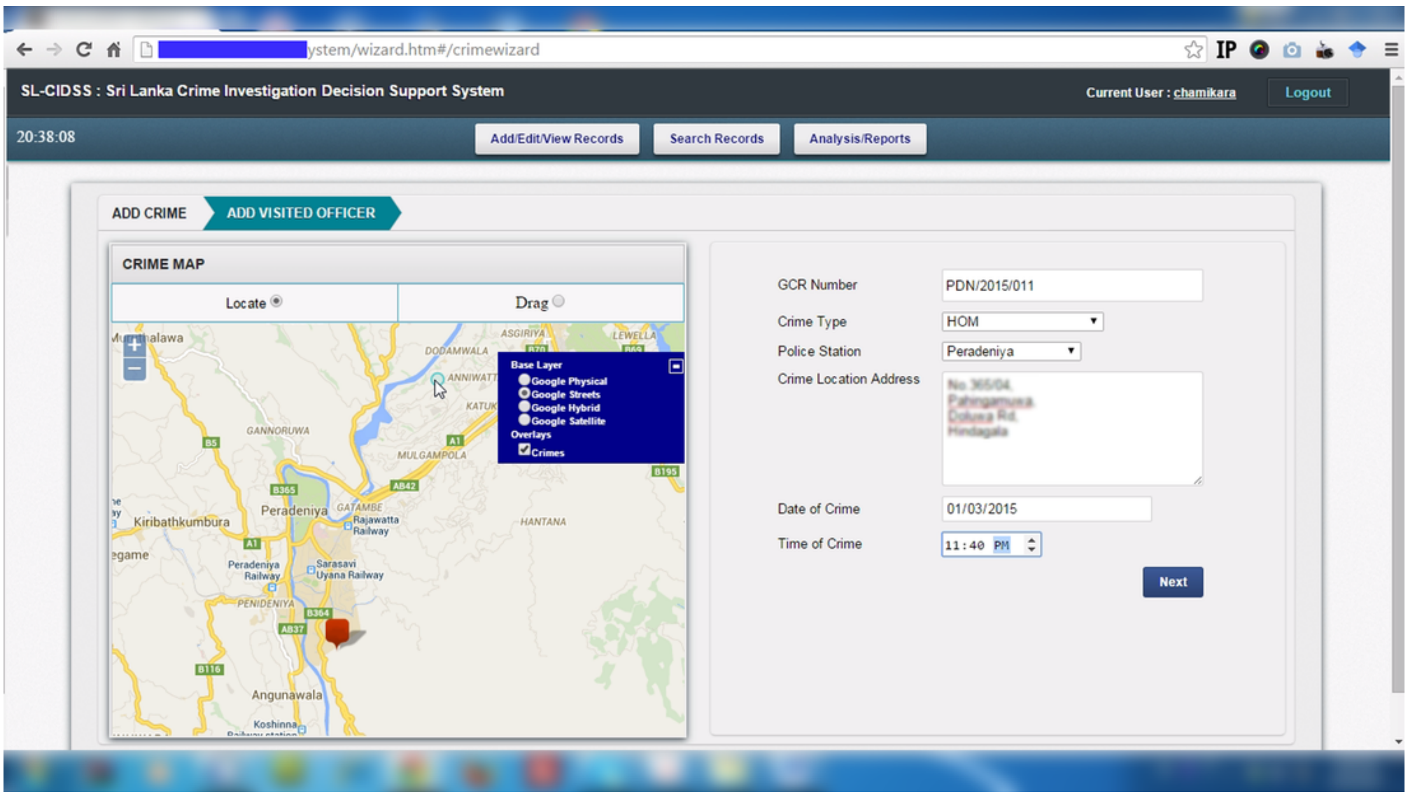


Fig. 14. A composite view in SL-CIDSS that includes a left sided map with a form used in inserting information.

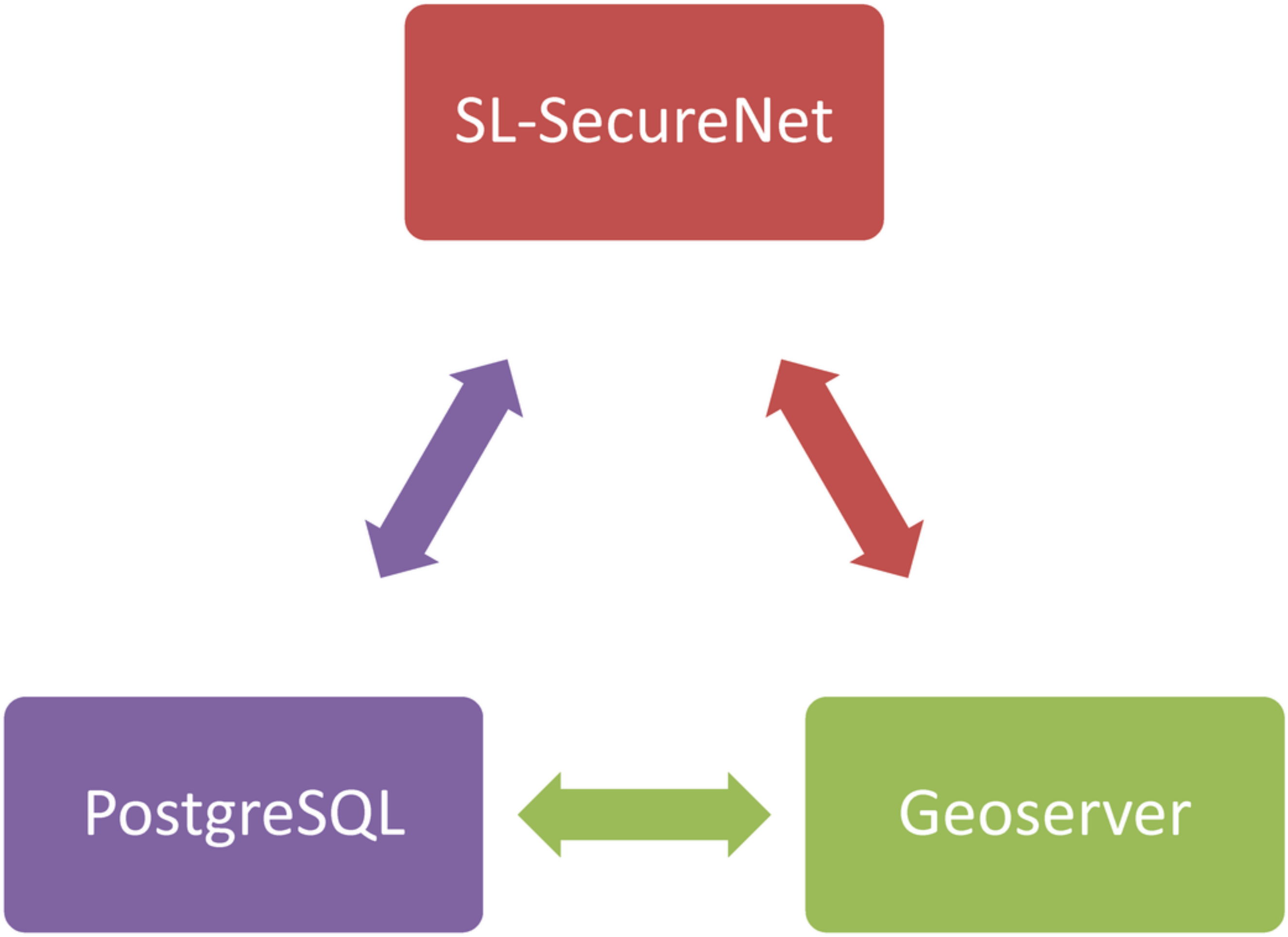
The map is used to locate a crime which is denoted by a red colored annotation. The form available in the right-hand side of the window is used to insert the information related to crime which is located on the map.



15

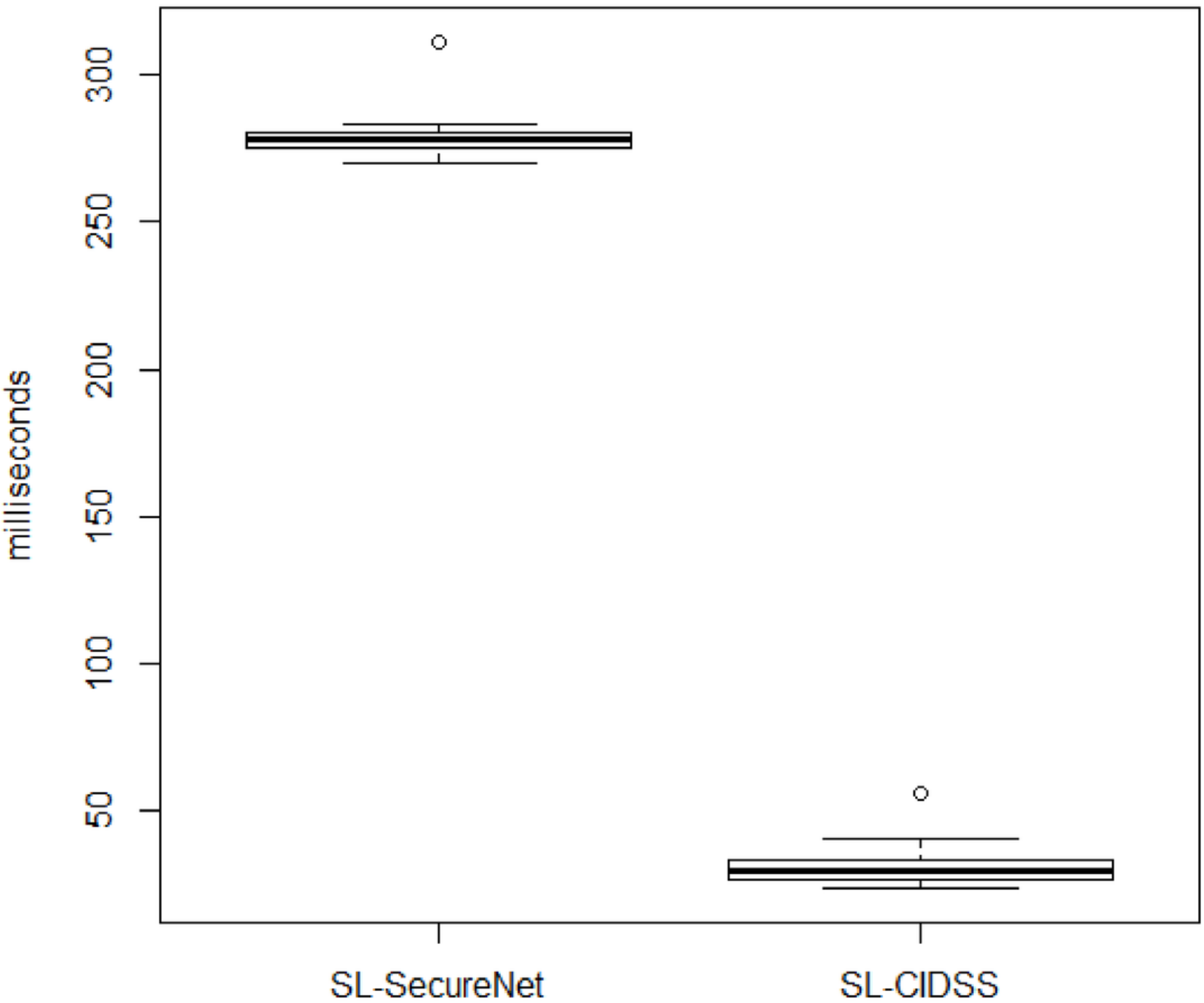
Fig. 15. SL-SecureNet information retrieval related to geographical and non-geographical data.

When SL-SecureNet wants to render geographical information on the maps, the communication with the PostgreSQL database has to be done through the Geoserver. Non-geographical data can be retrieved by the direct communication with the PostgreSQL database.



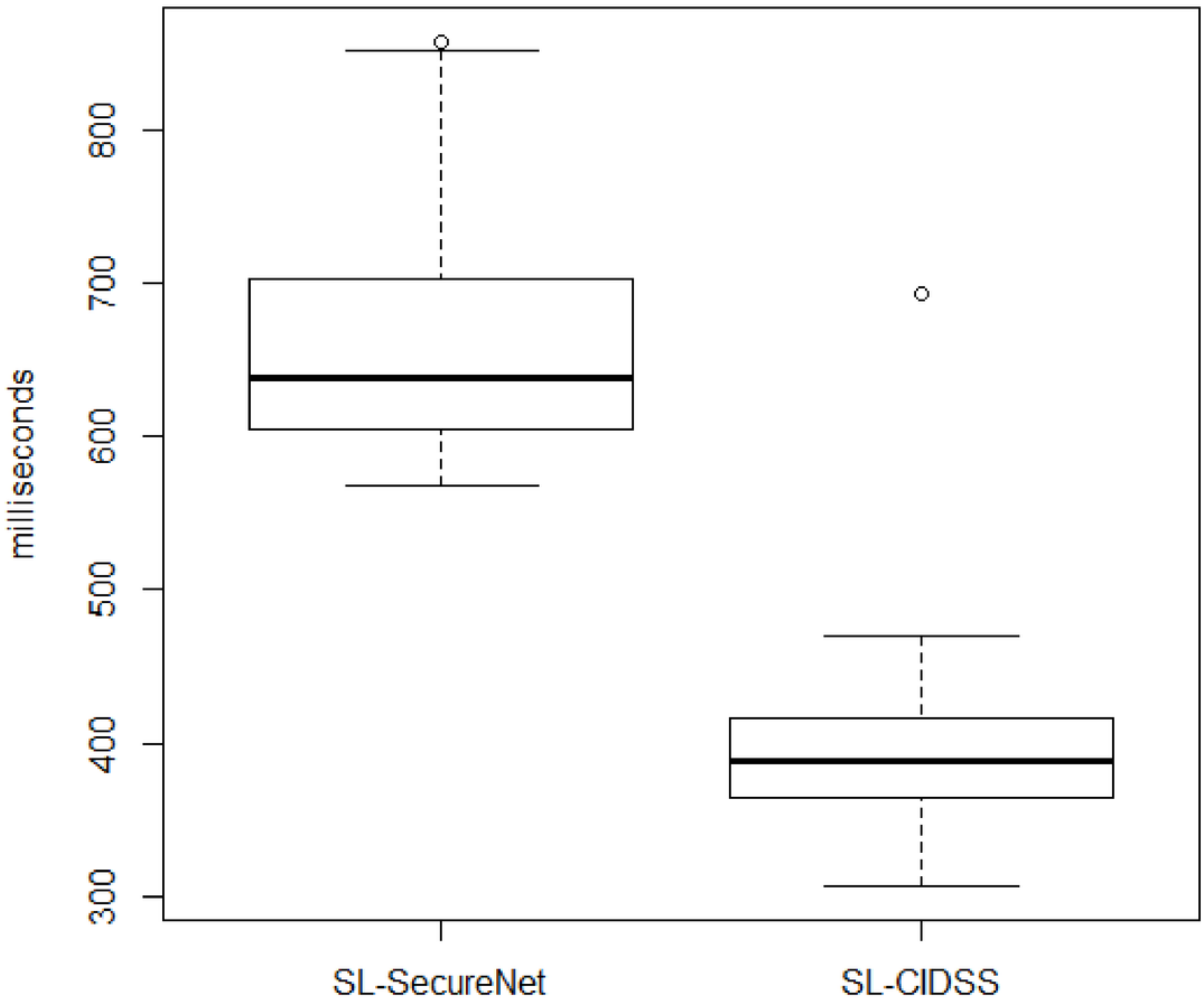
16

Fig. 16. Box plots for the processing time of System A and B for Task 1



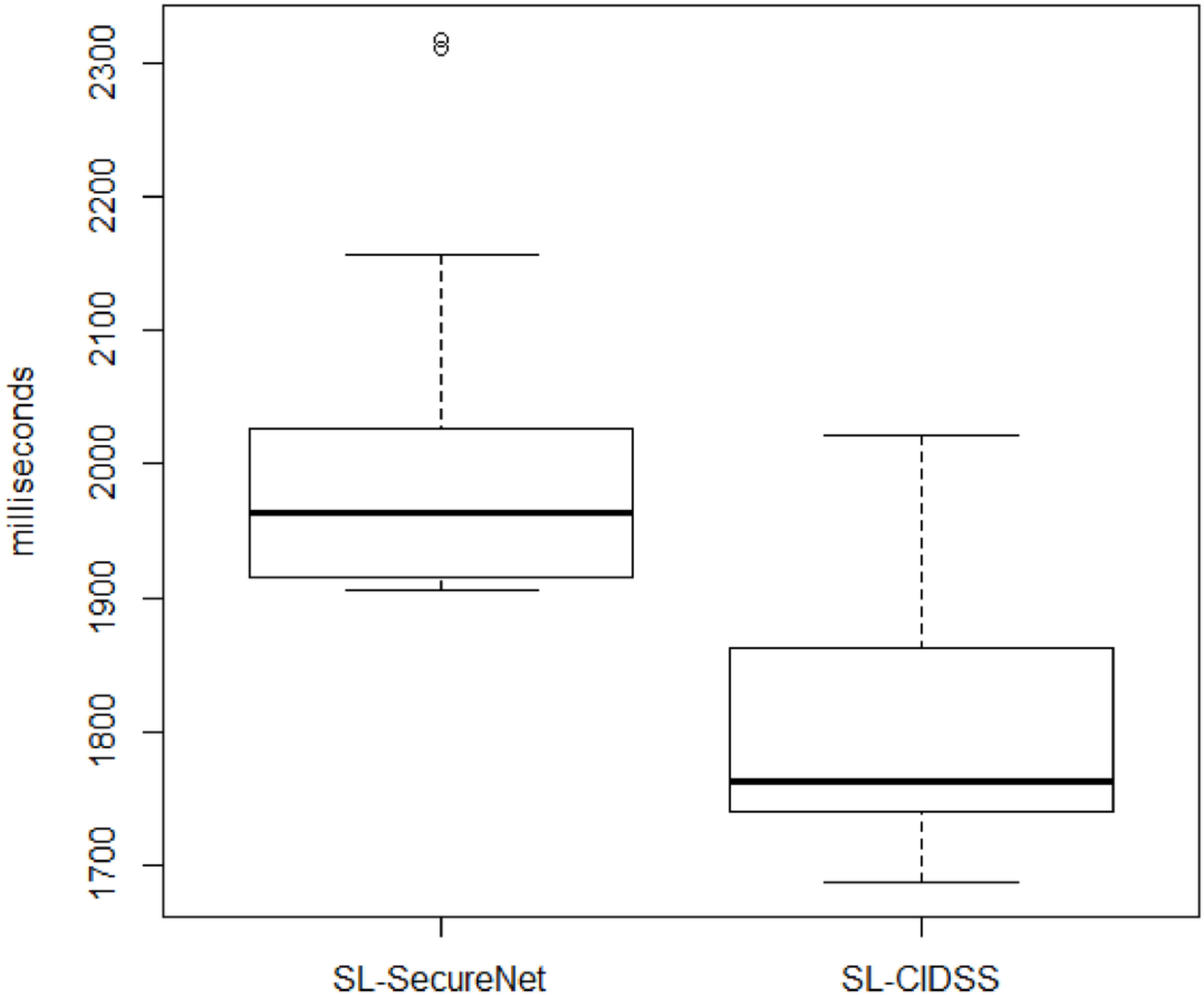
17

Fig. 17. Box plots for the processing time of System A and B for Task 2



18

Fig. 18. Box plots for the processing time of System A and B for Task 3



19

Fig. 19. Box plots for the processing time of System A and B for Task 4