TRUST ESTIMATION OF REAL-TIME SOCIAL HARM EVENTS

by

Saurabh Pramod Pandey

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer Science

Indianapolis, Indiana

August 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Rajeev R. Raje, Chair

Department of Computer and Information Science

Dr. George Mohler

Department of Computer and Information Science

Dr. Mihran Tuceryan

Department of Computer and Information Science

Approved by:

Dr. Shiaofen Fang

Head of the Graduate Program

Dedicated to my Amma and Babu.

ACKNOWLEDGMENTS

It gives me immense pleasure in presenting this thesis report titled: “TRUST ESTIMATION OF REAL-TIME SOCIAL HARM EVENTS”. I am sincerely thankful to my Advisor and Mentor, Dr. Rajeev R. Raje, for providing various perspectives for broadening my research along with his guidance and support. I would like to thank my Advisory Committee members, Dr. George Mohler for helping me with the Machine Learning component of this thesis and Dr. Mihran Tuceryan, for his insightful comments and encouragement. Additionally, I would like to thank Dr. Jeremy Carter for sharing social harm dataset and helping me in understanding the data through his expertise of Criminology domain.

I would also like to express my gratitude to my colleagues Milan Patil and Nahida Chowdhury for their assistance throughout this project.

I am thankful to IUPUI and the Department of Computer and Information Science for offering me the Dean’s Scholarship and continued support that allowed me to carry out my research successfully.

Last but not the least, I would like to thank my parents and my entire family for their encouragement and support throughout my master's journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Author: Pandey, Saurabh, P. MS
Institution: Purdue University
Degree Received: August 2019
Title: Trust Estimation of Real-Time Social Harm Events
Committee Chair: Rajeev R. Raje

Social harm involves incidents resulting in physical, financial, and emotional hardships such as crime, drug overdoses and abuses, traffic accidents, and suicides. These incidents require various law-enforcement and emergency responding agencies to coordinate together for mitigating their impact on the society. With the advent of advanced networking and computing technologies together with data analytics, law-enforcement agencies and people in the community can work together to proactively reduce social harm. With the aim of effectively mitigating social harm events in communities, this thesis introduces a distributed web application, Community Data Analytic for Social Harm (CDASH). CDASH helps in collecting social harm data from heterogenous sources, analyzing the data for predicting social harm risks in the form of geographic hotspots and conveying the risks to law-enforcement agencies. Since various stakeholders including the police, community organizations and citizens can interact with CDASH, a need for a trust framework arises, to avoid fraudulent or mislabeled incidents from misleading CDASH. The enhanced system, called Trusted-CDASH (T-CDASH), superimposes a trust estimation framework on top of CDASH. This thesis discusses the importance and necessity of associating a degree of trust with each social harm incident reported to T-CDASH. It also describes the trust framework with different trust models that can be incorporated for assigning trust while examining their impact on prediction accuracy of future social harm events. The trust models are empirically validated by running simulations on historical social harm data of Indianapolis metro area.

CHAPTER 1. INTRODUCTION

Humans, being a part of society, interact and share a relationship with nature and one another. These interactions pave way towards diverse social formations resulting in the establishment of lawful processes within the society [1]. Nevertheless, these interactions can become harmful. Pemberton [2] offers an explanation on when a social formation can become harmful: “[A]n individual is harmed through the non-fulfilment of their needs”. Such a non-fulfilment of needs leads towards social harm incidents in the society. Social harm is “a concept that enables criminology to move beyond legal definitions of ‘crime’ to include immoral, wrongful and injurious acts that are not necessarily illegal” [3]. This thesis proposes the use of technology to mitigate social harm incidents through efficient utilization of law-enforcement resources in the society.

1.1 Social Harm

Social harm, as the name suggests, includes incidents that cause socio-economic harm to the society. Thereby, along with legally defined criminal activities, social harm also includes incidents involving physical, financial, and emotional harms such as drug overdoses and abuses, traffic accidents, and suicides. It encompasses any incident causing damage to the society irrespective of it being intentional or not. Thus, Hillyard and Tombs [3], consider social harm more responsive to causes of human suffering than legally defined crimes.

1.2 Impact of Social Harm

One way of quantifying the impact of social harm is by estimating the economic burden borne by the society due to such incidents. Social scientists view costs associated with crimes in two aspects, tangible and intangible costs [4]. Tangible costs refer to direct monetary cost to the society including loss in business, damage to property, medical expenses etc. Intangible costs include psychological impacts resulting in fear and loss of productivity among victims. In this research, one key observation from the social harm data (2012-2013) provided by the Indianapolis Metropolitan Police Department (IMPD) for Indianapolis metro area was that the social harm incidents incurred approximately $1,980,567,045 cost to Indianapolis in 2012-2013 [5]. This indicates that heterogeneous social harm events, including crimes such as robbery, assault, homicides, etc., along with traffic crashes and drug abuses, affect communities adversely and police, fire, health, and social service departments must work together to prevent and mitigate such harms.

1.3 Dealing with Social Harm

Researchers and police departments have proposed various ways to alert communities about social harm events. Weisburd and Eck [6] discuss four different approaches to policing including the Standard Model of policing, Community policing, Hotspots policing, and Problem-oriented policing. They use research evidences for measuring the effectiveness of these approaches on three dimensions: reducing crime, disorder and fear in the community. They present that proactive policing strategies such as Hotspots policing, and Problem-oriented policing prove to be most effective on all three dimensions followed by collaborative strategy such as Community policing which only helps in reducing fear among citizens and lastly reactive strategy such as Standard Model of policing which seems to be most ineffective for dealing with crimes. One way of proactive policing is through geographic profiling [7] – it helps to analyze regions with connected crimes to identify likely areas of offender's residence. Also, data mining, machine learning, and software tools are being used for predicting social harm. A lot of research work has been conducted to utilize machine learning in crime prediction. McClendon and Meghanathan, in [8], have compared different machine learning algorithms, such as Linear Regression, Additive Regression, and Decision Stump, on violent crimes data for their effectiveness in crime prediction. Kiana et al., in [9], have used data mining techniques, such as clustering and classification, for discovering, investigating and analyzing patterns for occurrence of different crimes. Wang et al., in [10], proposed forecasting of crime in near real-time using the spatio-temporal deep learning technique. These prevalent approaches are, however, limited to few crime types and data sources. They may lead to a limited view towards efficient social harm policing in the society. Additionally, none of them takes into consideration the trust associated with data (either historical or live) being fed to the prediction models. Trustworthiness of the data may affect the prediction accuracy of the crime predicting model(s).

1.4 Motivation

Identifying high-risk areas helps the authorities to employ their resources efficiently – this approach seems to be the important next step in social harm prediction and "predictive policing". The "routine activities" approach is a leading sociological theory based on the premise that criminal events result from interactions between likely offenders and suitable targets occurring non-randomly in space and time [7]. Finding patterns of social harm using the historical data and clubbing it with live events reported by people living in the community can help in reducing social harm events.

Additionally, not much research has been conducted in interrelating 911's call for service data with the post investigating data relating to social harm. Such an interrelationship can help in analyzing social harm patterns in the society. By analyzing these patterns, false social harm alarms can be reduced thereby leading towards optimal allocation of law-enforcement resources.

Lastly, encouraging participation from various sections of the society can help in proactively reducing social harm. To achieve this, there is a need for a platform where various stakeholders including law-enforcement agencies, community organizations and citizens can easily and anonymously report live social harm incidents.

With these in consideration, this thesis proposes a platform for collecting and analyzing social harm events.

1.5 Overview of Proposed Approach

The specific objectives of this thesis are:

- To generate social harm hotspots and associated recommendations for directed and predictive policing, on a periodic basis, using historical and live social harm data.
- To associate trust with each live social harm incident and use it in the predictive modeling.
- To empirically evaluate the proposed approaches using the data provided by the IMPD.

To achieve these objectives, firstly, a distributed web application, Trusted Community Data Analytics for Social Harm (T-CDASH) is created. T-CDASH helps in generating social harm hotspots and communicating risks to law-enforcement agencies while allowing interactions with various stakeholders including the police, community organizations and citizens. It also helps in providing recommendations for performing specific actions to police officers while patrolling in the areas indicated as hotspots. Feedback from patrolling officers are also fetched in real-time. Along with this, real-world social harm records are collected, analyzed and preprocessed for generating hotspots. Lastly, a trust framework consisting of multiple trust models is developed, to assign a degree of trust with each social harm record. Eventually, the trust models are empirically validated and compared for their accuracy.

1.6 Audience

The core focus of this thesis is to assign trust with live social harm events. The trusted incidents are considered for predicting social harm hotspots. Also, as mentioned before, there are various stakeholders associated with the system including the police department, community organizations and citizens. Although there are many stakeholders, currently, the hotspots are utilized only by the police department for efficient allocation of patrolling officers. Having an efficient trust framework in place will result in having a higher degree of trust over the hotspots generated. This in turn will benefit the patrolling officers as it will ultimately provide them with hotspots which can be highly trusted thereby leading towards efficient patrolling.

1.7 Organization

This thesis is organized in five chapters. The first chapter introduces the aim of the thesis followed by the motivation and overall approach. The second chapter presents related research work in the social harm domain. The third chapter provides the architecture of the proposed system along with the design of trust framework with various trust models for associating a degree of trust with social harm events. Additionally, it describes the social harm data from multiple sources together with its preprocessing and interrelationships for evaluating the trust models. The fourth chapter compares the performance of the trust models while analyzing the impacts of empirical estimations within the system. Finally, chapter 5 discusses the conclusions and provides directions for future work.

CHAPTER 2. RELATED WORK

This chapter discusses related research efforts from the domain of social harm detection, prediction, and prevention. It also discusses the importance and techniques for incorporating ‘trust’ in distributed software systems.

2.1 Social Harm Prediction and Prevention

In today’s society, as observed by Greene [11], the role of police has evolved from just dealing with violent crimes to dealing with social harm incidents such as vehicles crashes, vandalism, and drug overdoses [12][13]. In the context of this observation, a lot of research has been carried out to analyze and predict social harm incidents in the society. Foot patrolling has been long considered a “proactive, non-threatening, community-oriented approach to local policing” [14]. Field surveys conducted in Philadelphia, Kansas City and New Jersey [15-19] depicted that foot patrolling did not have much impact in reducing crimes. Researches have shown that directed and proactive policing can contribute significantly in reducing crime and social harm incidents [20-25].

2.2 Social Harm Data

This thesis considered data from three different sources: Computer Aided Dispatch (CAD), Records Management System (RMS) and Uniform Crime Reporting (UCR). As explained by Law Enforcement Information Technology Standards Council (LEITSC) in [26], the CAD system assists in performing public safety operations in an automated manner. It includes incident reporting, emergency vehicle dispatch along with incident tracking and management capabilities. Information captured by CAD later assists in creating RMS reports. LEITSC [27] describes RMS as an agency-wide system for recording, persisting and retrieving information and documents related to law enforcement operations. Although RMS allows multiple incident reporting mechanisms, it records only a single entry for each incident. UCR, on the other hand, consists of data collected from four systems: The National Incident-Based Reporting System (NIBRS), the Summary Reporting System (SRS), the Law Enforcement Officers Killed and Assaulted (LEOKA) Program, and the Hate Crime Statistics Program [28]. This data is used by law enforcement agencies for administrating and managing social harm incidents. All the above systems help in maintaining the entire lifespan of an incident right from its initial reporting to its completion. Although these systems help immensely in tracking and analyzing social harm incidents in the society, limited work has been done in establishing any kind of interrelation between them. Such an interrelationship will help in reconciling the social harm incidents reported to the police with the incidents investigated and officially recorded by them. A unique contribution of this thesis is the interrelationship that it establishes between these systems for analyzing the incidents that are common between them.

Since social harm data is a time series data, time series data validation was performed on the social harm records. Data cross validation was performed to analyze its impact on the performance of various trust models of T-CDASH. Tashman [29] proposed various techniques including Fixed Origin, Rolling Origin, and Rolling Windows for selecting in-sample data for training the prediction module. In Fixed Origin, the origin remains fixed at a particular period, T, while predictions are generated for periods T+1, T+2, … T+N. Since the origin remains fixed, this technique is prone to errors due to data unique to the origin. Rolling Origin, on the other hand, considers multiple origins by increasing the in-sample data in each forecasting iteration. This helps in alleviating the concerns related to Fixed Origin. Rolling Windows are similar to Rolling Origin but maintain constant in-sample size by pruning oldest records. Pruning helps in clearing old data thereby helping in updating model coefficients. This thesis has used Rolling Origin and Rolling Windows techniques for analyzing their impact on hotspot predictions.

2.3 Statistical Modelling and Machine Learning in Social Harm Domain

Plenty of research work has been carried out in utilizing software tools for predicting and mitigating social harm in the society. Multiple machine learning techniques have been used for analyzing and predicting crime and social harm along with software applications for reporting and displaying live crime events. A lot of literature is also available on the use of machine learning and data analysis to predict social harm hotspots and patterns. Various machine learning and data mining algorithms (as indicated below) are applied, in order to gain insights of different types and sources of crime and social harm.

Bogomolov et al. [30] used demographics and mobile data for predicting crimes. They used human behavioral data in the anonymized form derived from demography and through mobile phone activity together with open crime data of London metropolis. Random Forest algorithm was used to predict whether a geographic location will be a crime hotspot in the next month or not. They achieved 70% accuracy in their crime predictions. However, one of the limitations of their work was availability of data. The data was aggregated on monthly basis leading to predicting crimes for next month rather than predicting for next week, day, or hour.

Yu et al. [31] have utilized temporal, spatial, societal, and ecological factors in forecasting crime. They designed and developed a Cluster-Confidence-Rate-Boosting (CCRBoost) algorithm to analyze historical crimes in the spatio-temporal domain and generate spatio-temporal patterns based on them. They used January 2006 to December 2009 crime data of a northeastern US city obtained through a police department. They evaluated their algorithm on the residential burglary crime type and found it to achieve an impressive 80% accuracy in predicting future residential burglaries. However, the algorithm was evaluated only on a single crime type leaving a question about its usability with multiple crime types clubbed together.

Chen et al. [32] performed sentiment analysis on the Twitter data; combining it with weather and historical crime data for predicting future crimes. They gathered the Twitter data of Chicago area from January 1 to January 31, 2014. Chicago's weather data was obtained from the Weather Underground website. They also utilized the historical theft data obtained from the Chicago Police Department collected from December 25, 2013 to January 31, 2014. Sentiment analysis was performed on this dataset by applying lexicon-based methods combined with Kernel Density Estimation and linear modelling for forecasting thefts. Their approach was able to capture approximately 42% crime with about 20% area of Chicago under consideration. However, in their work, they did not specify any direct connection between tweets and specific crime types. Also, the authenticity of tweets was not considered.

Mohler et al. in [5] proposed a modulated Hawkes process for indexing social harm incidents. The indexing was based on the expected cost of the incidents towards the community. This index was utilized while ranking the hotspots over time for their significance. They obtained social harm data including crimes, drug overdoses, and vehicle crashes from various government agencies such as the Indianapolis Metropolitan Police Department (IMPD), the Indianapolis Emergency Medical Services, and the Indiana State Police using the Automated Reporting Information Exchange System (ARIES) for 2012-2013. Hawkes process forecasted crime through an intensity function based only on historical social harm events which modelled long term intrinsic and short-term dynamic risks and estimated trends. Hawkes process, as proposed, captured approximately 20% of social harm cost in about 2% of space-time.

This thesis utilizes the Hawkes process model as proposed in [5] for predicting social harm incidents and generating hotspots.

2.4 Trust

An important aspect in predicting future by analyzing current and historical events is the trustworthiness of the available data. In order to generate reliable predictions, it is important for the data to be credible – i.e., there is a need to consider the trust associated with the data. Accordingly, while predicting social harm with data from heterogeneous sources, it is necessary to associate trust with each social harm incident used in predictions. Association of trust will help in reducing misleading and/or fraudulent social harm reports along with any data recording inaccuracies. Researchers have done a lot of work for estimating trust in distributed software environments. Jøsang [33] introduced a framework based on an opinion model and subjective logic for associating trust with events. Subjective logic views any proposition as not being either true or false but rather on the basis of subjective belief (*b*), disbelief (*d*) and ignorance/uncertainty (*i/u*). That is, opinions regarding a proposition translate in varying degrees of belief, disbelief and uncertainty. The belief, disbelief and uncertainty are calculated based on evidential reasoning. For any proposition, positive evidences supporting the proposition contribute towards high belief. Similarly, negative evidences opposing the proposition contribute towards high disbelief. Since, each proposition can have multiple opinions, subjective logic provides various operators, including Conjunction, Disjunction, Negation, Recommendation, and Ordering, for combining the opinions. This thesis uses the concept of the opinion model for assigning certain degree of belief, disbelief, and uncertainty to each social harm incident before utilizing them for hotspot predictions.

Ceolin et al. [34] have designed a trust algorithm based on Subjective Logic as indicated by Jøsang in [33]. They applied the algorithm to a use case for tracking ships in maritime domain. The algorithm calculated the level of belief, disbelief and uncertainty associated with each event as follows:

$$b = \frac{positive\_evidence}{total\_evidence + n}$$

$$d = \frac{negative\_evidence}{total\_evidence + n}$$

$$u = \frac{n}{total\_evidence + n}$$

$$a = \frac{1}{n}$$

In this, *b, d, u* were the degree of belief, disbelief and uncertainty respectively and *a* was the probability that proposition was true in the absence of evidence (a priori probability) and *n* was number of the possible outcomes. This thesis uses a similar approach in the domain of social harm prediction for associating trust with social harm incidents. For each incident, belief, disbelief, and uncertainty are computed (using the above formulae) taking various factors into consideration as described in Chapters 3 and 4.

Another popular way of associating trust with events is through the reputation model. As per Wikipedia, “Reputation systems are programs that allow users to rate each other in online communities in order to build trust through reputation.” [35]. Furtado et al. [36] describe the WikiCrimes system and the trust management mechanism incorporated within it. They have depicted WikiCrimes as a platform for reporting and analyzing live crime incidents. In their work, they have presented ways for allowing a high degree of people participation, while maintaining high credibility of the information reported by the people. WikiCrimes builds a reputation model and uses the reputation score of the user while associating trust with the user-reported event. The users are registered in WikiCrimes with name and email addresses. As the events reported by a user gets verified by more and more other reputed users (e.g., law-enforcement entities), the reputation score and the credibility of the reporter increases. Also, trustworthiness of a reported information increases, the more it is confirmed. Thus, the reputation of a user is built through interactions. However, there are two key concerns with the reputation-based model in the social harm domain. First, maintaining user anonymity is pivotal in such a domain, as it can have serious consequences with respect to safety and security of incident reporters. The name and email address of the users, if compromised, can jeopardize their well-being. Second, the reputation score builds over time and a malicious user may build a reputation through less sensitive crime reporting while misleading the system in the event of a high severity crime. It was for these reasons, that this thesis did not incorporate reputation model but used other crime-related attributes such as location, days and incident types to associate trust with the reported incidents.

2.5 Previous Work

2.5.1 Community Data Analytics for Social Harm (CDASH)

As an initial effort, we have created a distributed web application, CDASH [37], with the aim of not only predicting social harm hotspots but also allowing various stakeholders including law-enforcement agencies, community organizations and citizens, to interact and report live social harm events to the system. A preliminary prototype accessible through desktops as well as hand-held mobile devices is developed as presented in [37]. Key features of CDASH include:

- Reporting live social harm events into the system.
- Periodic prediction of social harm hotspots.
- Dynamic communication of risks for efficient resource allocation.

CDASH is developed using the principles of Service Oriented Architecture (SOA) where each system functionality was fulfilled by a self-sufficient service. It consists of a layered architecture as depicted in Figure 2.1.

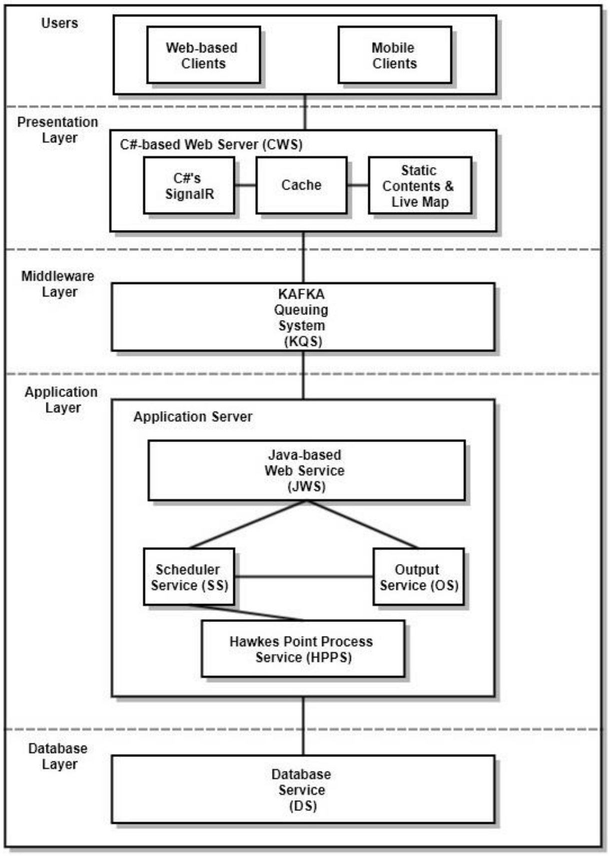


Figure 2.1: System Architecture of CDASH [37]

CDASH is built using the Model-View-Controller (MVC) software architectural pattern. Following layers are incorporated in CDASH.

Presentation Layer: The Presentation Layer of CDASH consists of a C#-based Web Server (CWS). It helps in enhancing system interactivity by presenting social harm information in a user-friendly manner. Two key components of the Presentation Layer are:

- **SignalR:** One of the key requirements with CDASH is to provide an ability to enter live social harm events in the system. Also, with every police shift, hotspots were to be updated by the HPPS. With these aspects in consideration, CDASH required a mechanism for dynamically updating all the clients connected to it. This capability is provided by the SignalR module of C#. Whenever a client is connected to CDASH, it automatically joins a hub created and managed by SignalR. Through this hub, SignalR maintains a list of clients connected to the system. Whenever any update occurs in CDASH, all the connected clients are dynamically updated. Also, whenever a client is disconnected from the system, it is automatically removed from the hub's notification list. SignalR implements the Observer software design pattern and ensures that the connected clients are always automatically updated with the most recent state of CDASH.
- **Static Contents and Live Map:** Static contents help in enhancing the user's experience while interacting with CDASH. It consists of HTML, Bootstrap, CSS and JavaScript along with its libraries (jQuery and AJAX). While HTML, Bootstrap and CSS help in enhancing the interactivity and user friendliness, JavaScript compliments the basic HTML functionalities along with providing a means for communicating with the web and application servers. Google maps are used to display hotspots and live incidents reported by the users. Any change in the state of CDASH is reflected dynamically on the live Google map.

Middleware Layer: Fault tolerance is one of the major challenges faced by any large distributed system. In CDASH, it is important for the prediction service to consider each live incident entered into the system. In situations when the backend components (services in Application and/or Database Layers) are unresponsive, it is necessary to avoid the loss of live incidents reported to the system. This is achieved through Apache's Kafka®. Kafka is a distributed queuing mechanism for receiving, storing and forwarding messages [38]. With CDASH, the Kafka Queuing Service

(KQS) is implemented using the publish-subscribe model. The Web Server behaves as a publisher, while the Application Server acts as the subscriber. The KQS holds live incidents, whenever backend is unresponsive, and forwards them automatically whenever the backend becomes responsive. Along with making the system fault tolerant, the KQS also ensures scaling of the CDASH system.

Application Layer: The Application Layer holds the business logic of CDASH. As stated above, this layer acts as a subscriber for KQS. Additionally, it comprises of various services and components, which fulfill different functionalities in the system. This layer includes the following services:

- **Java-based Web Service (JWS):** The JWS consists of various controller components, which are RESTful entry points for various functionalities into the system. All the user requests flow through the JWS towards the desired components and services thereby invoking the corresponding functionalities associated with the requests.
- **Duplication Handler:** Duplication hander, as the name suggests, is a component that identifies the duplicity of live social harm events reported to CDASH. When a social harm occurs, it is possible that it gets reported by multiple people to the system. When the system receives a live incident, this component, based on time, location and the incident-type, evaluates the incident for a possible duplication. This is necessary to avoid any confusion with display of duplicate events on the map.
- **Hawkes Point Process Service (HPPS):** The HPPS is a machine learning technique based on mathematical and statistical models as detailed in [5]. Written in MATLAB®, the HPPS is a self-exciting point process indicating the probability of occurrence of an event through an intensity function, based on the past events. It helps in modeling risks and forecasting trends in social harm. The risks are indicated in the form of social harm hotspots. These hotspots are geographic locations indicating high probabilities of certain social harm events occurring in near future.
- **Scheduler Service (SS):** Over a period, the live incidents reported to CDASH become historical and are fed to the HPPS for generating new hotspots. It is important to consider that the hotspots do not change with every single live incident that is reported to the system. Thus, it is necessary to invoke the HPPS periodically. Currently, SS runs once in every 24 hours and

invokes the HPPS to generate new hotspots taking into consideration all the historical incidents along with the ones reported in the previous day.

- **Output Service (OS):** Any change within the state of CDASH necessitates its reflection on the Google maps to keep the stakeholders updated. The OS helps in communicating these system changes to the Google map. Whenever, a change in the system state, such as an update of hotspots or reporting of live incident, occurs it is communicated to the Presentation Layer by the OS.

Database Layer: CDASH stores and utilizes demographic data of various geographic locations in Indianapolis that are utilized by the HPPS in generating hotspots. The Database Layer consists of a MySQL database and a Database Service (DS) that helps the application layer in interacting with the database. The database also records all the reported live social harm events. This allows CDASH to interrelate and filter out duplicate events reported to the system.

2.5.2 Experiments and Analyses with CDASH

Heterogeneity: CDASH is designed to handle hardware heterogeneity. As stated, in section 2.5.1, it is developed to work with desktop browsers as well as mobile handheld devices. It ensures that CDASH is accessible to large spectrum of users. Figure 2.2 displays the desktop view provided by CDASH.

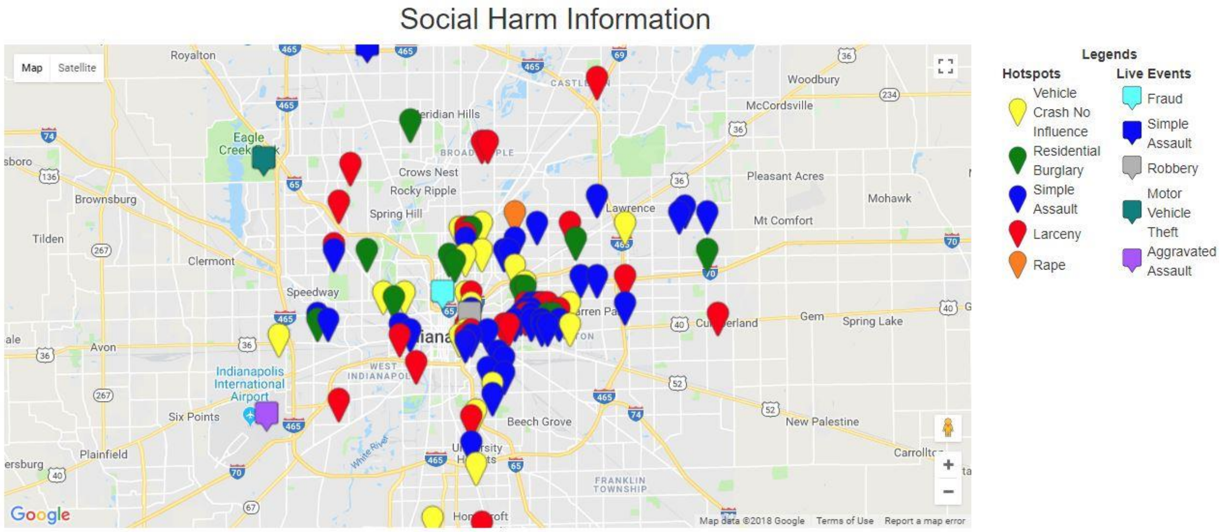
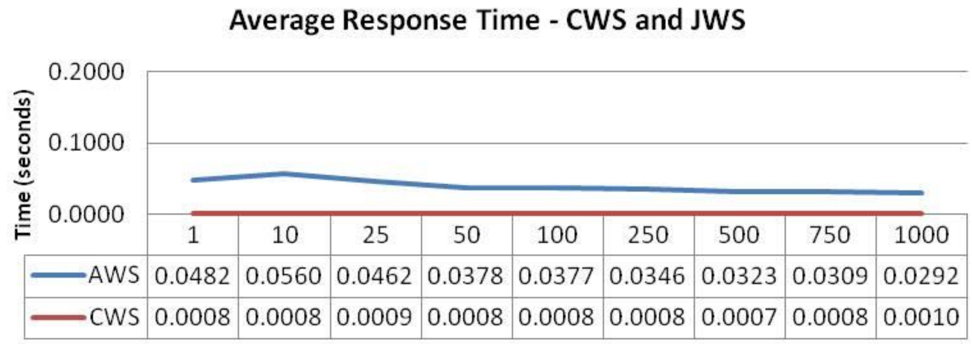


Figure 2.2: Social Harm Information

Scalability: Scalability of CDASH is measured by analyzing the average response time for varying amounts of concurrent requests. Since the front-end (Presentation Layer) and back-end (Application and Database Layer) of the system are decoupled, the response-time of Presentation and Application Layers were measured and analyzed separately. To simulate real-world scenario, different loads of concurrent requests (maximum of 1000) were used in the scalability experiments. The response time of Presentation Layer was found to be in the range of 0.86 milliseconds to 1 millisecond; while that for the Application Layer was found to be in the range of 29 milliseconds to 56 milliseconds - both these numbers are near real-time. With the Presentation Layer, it was observed that most of the time was taken for updating the map. With the Application Layer, JWS and DS took time to perform the business logic and persist data. Figure 2.3 depicts the performance CDASH achieved with various concurrent load of requests.



	1	10	25	50	100	250	500	750	1000
AWS	0.0482	0.0560	0.0462	0.0378	0.0377	0.0346	0.0323	0.0309	0.0292
CWS	0.0008	0.0008	0.0009	0.0008	0.0008	0.0008	0.0007	0.0008	0.0010

Figure 2.3: Average Response Time of CDASH

Fault Tolerance: With CDASH, fault tolerance is viewed with respect to three aspects: the CWS failure, the JWS or DS failure and the client failure.

- **CWS Failure:** Whenever CWS fails, the point of contact with the system is lost and an appropriate message of unavailability is shown to the user. This situation requires restarting of the CWS.
- **JWS or DS Failure:** When the JWS or DS fails, Kafka helps in achieving fault tolerance. Kafka holds the reported events in its server while the JWS or DS are unresponsive. Whenever the unresponsive components become available, Kafka automatically delivers the stored events for further processing. Additionally, two instances of JWS are configured to run in fault tolerant mode. Their synchronization is handled automatically by Kafka.

- **Client Failure:** In the event of the client failure, CDASH ensure that any event reported by the client is processed appropriately. Also, the client can see the most recent and updated view of the system once it reconnects with CDASH.

Accuracy: To analyze the accuracy of CDASH, simulations were run using 2012-2013 social harm data of Indianapolis metro obtained from the IMPD. 18 different categories of social harm incidents as indicated in [5] were considered in this study. It was observed that CDASH captured 20% of social harm cost in 2% of space-time.

This initial prototype of CDASH forms the basis of this thesis. This initial design is enhanced further to include additional functionalities such as role-based access, recommendations, feedback features, and trust models. These enhancements are discussed in Chapters 3 and 4.

2.6 Summary

As illustrated in this chapter, a lot of research work has been done in predicting crime or social harm incidents through various data mining and machine learning techniques. Also, there are applications, such as WikiCrimes [36], that allow reporting and analysis of live social harm incidents and associate trust with the reported incidents. However, limited work has been done in creating a comprehensive system that combines prediction of future social harm incidents while allowing users to report live incidents. Additionally, research has been conducted on exploring various ways of associating trust with live social harm incidents. However, merging the trust models into a comprehensive prediction system is needed – which is one of the goals of this thesis.

CHAPTER 3. PROPOSED APPROACH

This chapter describes the proposed approach for creating a predictive system to mitigate social harm. In addition to presenting the design of the proposed system, the chapter discusses various datasets used as input to the system. The second part of the chapter focusses on estimating trust by proposing and comparing multiple trust models for real-time social harm events.

3.1 Extension of CDASH Application

The proposed predictive system, called T-CDASH, is shown in Figure 3.1. T-CDASH enhances the CDASH system [37] described in the previous chapter. The additional/enhanced services and components included in T-CDASH are highlighted in Figure 3.1 and discussed below.

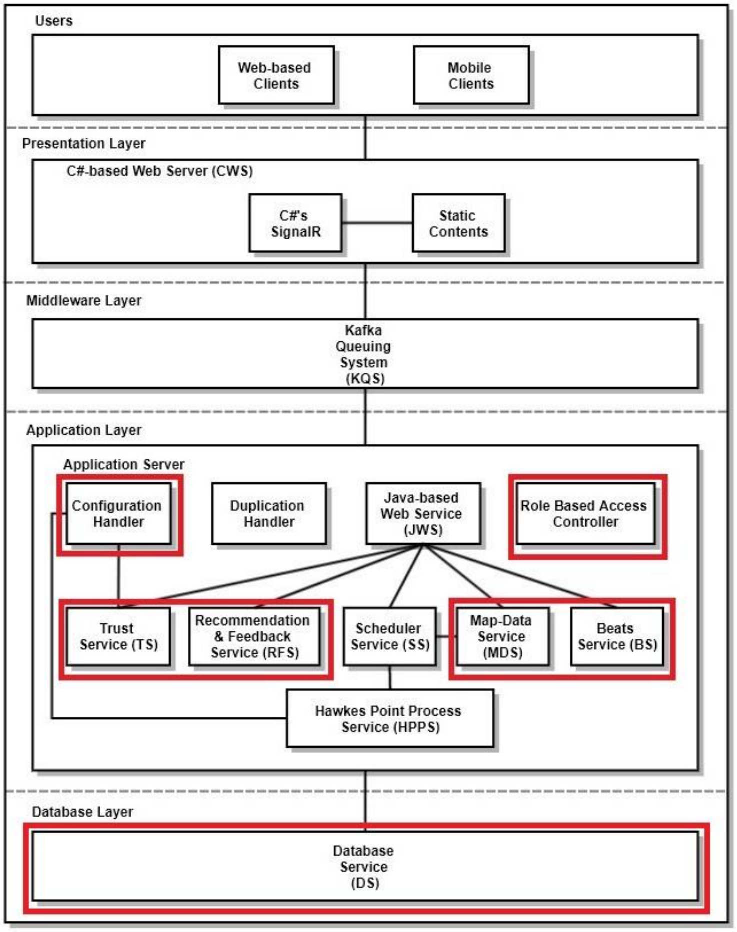


Figure 3.1: System Architecture of T-CDASH

Configuration Handler: The T-CDASH system comprises of various services that work together to fulfill functionalities provided by the system. Additionally, to make T-CDASH flexible, it is developed using the fundamentals of generative programming. With generative programming, it is possible to develop the system with a family of services that confirm to a defined interface. This allows a service to be selected at runtime. Thus, different services providing the same functionality can be a part of the system simultaneously. For example, currently T-CDASH has six different trust models including Ground-truth, Optimistic, Pessimistic, Random, Average and Opinion-based model. In future, each of these models can be converted into a self-sufficient service. The Configuration Handler will allow one of those services to be invoked at runtime. Also, it will allow the system- administrators to modify the type of service to be invoked at runtime without restarting the T-CDASH system.

Role Based Access Controller: Various stakeholders including the police department, community organizations, citizens and T-CDASH system-administrators interact with T-CDASH. This necessitated the use of role-based access for T-CDASH. It allows each stakeholder to view, access and interact only with the functionalities developed for the corresponding user. For example, currently, the police officers can view the live social harm events reported to T-CDASH along with the hotspots generated by T-CDASH. They are also displayed with hotspot-specific recommendations and can provide feedback regarding the actions taken while patrolling a hotspot. On the other hand, currently, citizens are only allowed to view the live social harm events reported to T-CDASH along with hotspots.

Trust Service (TS): One of the important aspects of T-CDASH is that it allows various stakeholders to interact with it. Hence, it is possible that some rogue individuals or organizations will attempt to mislead the predictions by providing fake data to T-CDASH. Also, inaccuracies may occur while reporting data reported to T-CDASH due to selection of incorrect incident category. To avoid such erroneous situations, the TS is introduced in the T-CDASH. Every live incident is assigned a trust value in the system (discussed later). Depending on the trust value, a decision is made whether the incident should be considered for prediction of social harm hotspots or not. This decision is based on various factors which are explained in the Trust Management Section (Section 3.4).

Recommendation and Feedback Service (RFS): Two additional key functionalities provided by T-CDASH are: providing recommendations and gathering feedback from the IMPD police officers. Every police department, such as IMPD, divides the area under its jurisdiction into several beats for better management of its resources. Each police officer is assigned a beat (patrolling area). Each beat covers a certain geographical area and has certain hotspots flagged within it. Depending on the hotspots within the beat, a set of three recommendations are provided to the police officers. These three recommendations are customized for each hotspot and are based on the most desirable actions taken by the police officers while patrolling. However, sometimes, it is conceivable that the police officers may take other actions as demanded by the situation. This scenario requires a means to understand how frequently the recommendations will be accepted by the police officers. Thus, RFS service contains a mechanism to record whether the recommendations are helpful to the police officers or not. These tasks of creating and displaying recommendations and gathering feedback from police officers is handled by the RFS.

Beats Service (BS): Currently, IMPD has divided the area of Marion County into 78 different beats. Officers police and patrol only within the beat assigned to them. Boundary-related information of these beats is stored in T-CDASH in the form of Keyhole Markup Language (KML) [39]. In future, the area and number of beats may change. Thus, it is necessary to allow these modifications seamlessly within T-CDASH. The Beats Service is created to store, retrieve and modify the information of beats under consideration.

Map-Data Service (MDS): Any event occurring in T-CDASH must be reflected on the Google map to keep the stakeholders updated. MDS helps in communicating these updates to the map. Whenever, new events such as update of hotspots, report of events, display of recommendation or feedback from police officers occurs, the user-interaction with T-CDASH is handled by the MDS. This service is available in the earlier prototype as detailed in [37] under the name of Output Service (OS) and is renamed to indicate its functionality more appropriately.

Also, the Database Layer of CDASH is modified to incorporate the above-mentioned functionalities. Table 3.1 presents the database schema for T-CDASH.

Table 3.1: Database Schema for T-CDASH

Table	**Description**
HppsInput	Stores the historical social harm incidents data, utilized by HPPS to generate social harm hotspots.
HppsOutput	Stores the hotspots generated by HPPS.
Demography	Stores the demographic information of various locations in the Marion county. This information is used by HPPS while generating hotspots.
County	Stores information related to a county including its name, KML and corresponding GeoJSON (A format for storing KML data).
Beats	Stores the name and geographical coordinates of beats.
Live_Incidents	Stores all the live events reported by various stakeholders of the system.
Recommendations	Stores three recommendations corresponding to each type of social harm incident.
Feedback	Stores the feedbacks provided by patrolling officer.
Police_Beat	Stores data that helps in identifying the beat assigned to police officers.
Beat_Prediction_Count	Stores information of hotspots along with their associated beat.
Users	Stores information of all the users registered with T-CDASH along with their roles.
Access_Policies	Stores the access policies associated with each role in T-CDASH.
CAD	Stores the CAD data provided by IMPD.
RMS	Stores the RMS data obtained from Socrata.
UCR	Stores the UCR data provided by IMPD.
CADMapping	Stores mappings to convert CAD incident types to T-CDASH incident types.
RMSMapping	Stores mappings to convert RMS incident types to T-CDASH incident types.
UCRMapping	Stores mappings to convert UCR incident types to T-CDASH incident types.

Additional Features:

- **GeoJSON**: GeoJSON is a format for displaying geographical features on maps [40]. It is an open standard based on JavaScript Object Notation (JSON) format. In T-CDASH, two key geographic features are identified: beats and hotpots. The geographic information related to beats is provided by the IMPD in the Shapefile format. Shapefile is a geospatial vector data format for representing geometric features such as points, lines and polygons stored in Geographic Information System (GIS) file format [41]. GIS files are created by governmental agencies for encoding geographical information [42]. Keyhole Markup Language (KML), developed by Google, is an XML-based notation for displaying and visualizing geographic information and features on maps [39]. Since it is easier to work with KML format than the encoded Shapefile format, the Shapefile is converted to KML using ArcGIS tool [43].

- **Toggling Beats and Hotspots**: One of the features required by the IMPD is an ability to toggle beats and hotspots on the map. This allows the patrolling officers to view either only the beat information or the hotspots information or both. This feature is achieved by providing a toggle button for beats and hotspots.
- **Beat-specific Hotspots**: An important feature of T-CDASH is the beat-specific display of hotspots. Each patrolling police officer is assigned to a beat. It is necessary to display only the hotspots associated with the beat of the officer. The beat-specific hotspot display allows the officers to view and analyze hotspots only associated with their beat.

3.2 System Flow

3.2.1 Live Event Flow

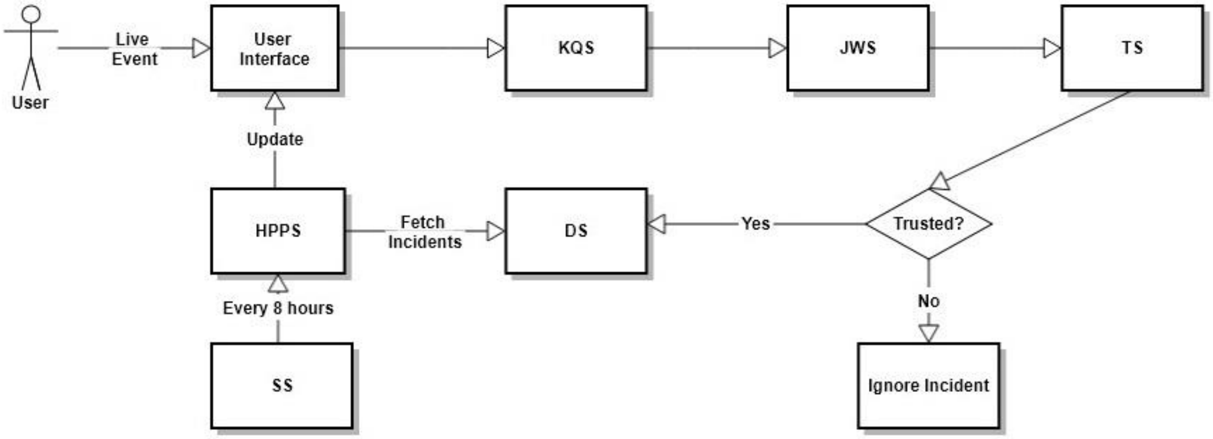


Figure 3.2: Live Event Flow

Figure 3.2 depicts the journey of a live event reported by a user. The user can report an incident through T-CDASH's user interface, and the interface is immediately updated to reflect the reported incident. Simultaneously, the reported incident is passed on to the Kafka's Queuing Service (KQS). Kafka forwards the incident information to the Java's Web Service (JWS) as indicated in Figure 3.2. JWS first passes the incident to a Trust Service (TS) that assigns a certain degree of trust to the incident. Once a trust value is assigned, a decision is made to either process or ignore the reported incident. The incident is ignored if the belief (see the discussion in Section 3.4) associated with incident is below a certain predefined threshold value (a parameter that can be adjusted). Otherwise, the incident is enriched with the demographic information of the location where the incident occurred and is stored using the Database Service (DS). Currently, after every 24 hours, a Scheduler Service (SS), automatically invokes the Hawkes Point Process Service (HPPS) – the HPPS is a machine learning service that helps in generating social harm hotspot. It fetches all the incidents stored in the database and generates the new hotspots, which are presented to the users.

3.2.2 Recommendations Flow

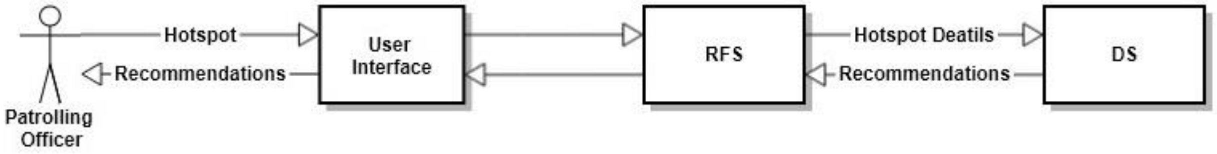


Figure 3.3: Recommendations Flow

Figure 3.3 depicts the process of fetching recommendations for the patrolling police officers. Each police officer, as indicated earlier, is assigned to one patrolling beat. The officer is presented with the beat information along with the information of hotspots within it – currently, the top three hotspots (with respect to average cost) within the beat are displayed. Each hotspot represents top three type of incidents that are most likely to occur within the hotspot area. Depending on the hotspot's incident types, recommendations are generated and presented to the officer. These recommendations suggest the most likely actions previously taken by the patrolling officers while patrolling for similar incidents. When an officer clicks on a hotspot, the information is passed on to the Recommendation and Feedback Service (RFS). The RFS invokes the DS for fetching a set of top three recommendations depending on the hotspot information. These recommendations are then presented to the patrolling officer.

3.2.3 Feedback Flow

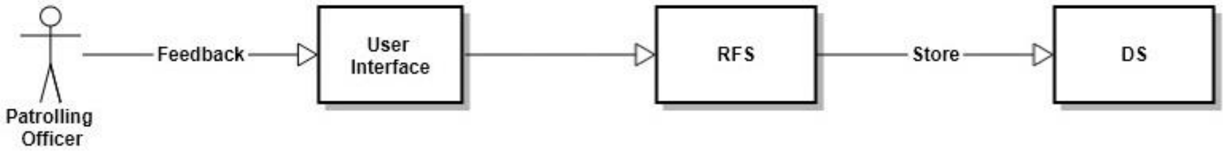
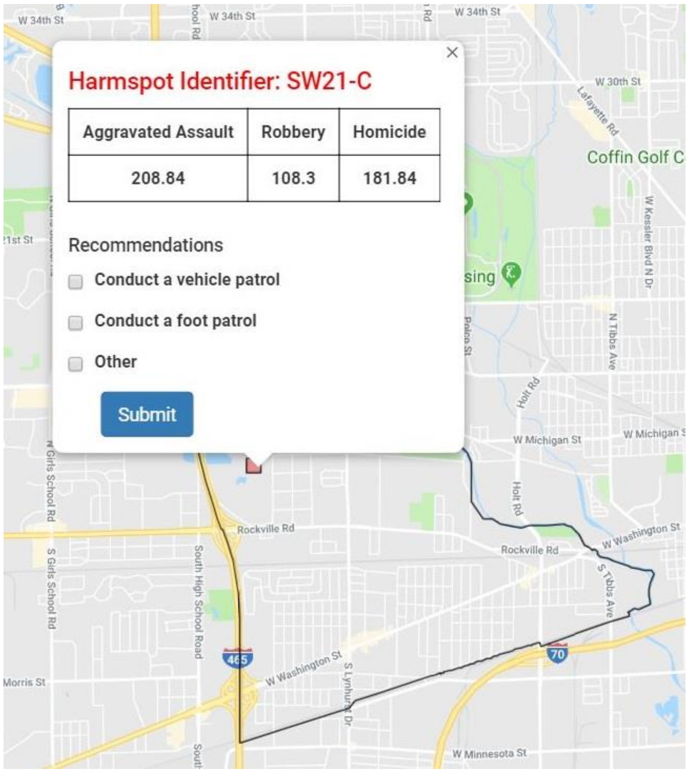


Figure 3.4: Feedback Flow

Figure 3.4 displays the process of capturing feedback from the patrolling officers regarding the recommendations provided to them. Section 3.2.2 explains the process of providing hotspot-specific recommendations to the police officers. Once the recommendations are provided, it is necessary to assess the usefulness of these recommendations to the police officers. Hence, T-CDASH allows an interactive interface which enables the officers to select the list of recommendations they found to be useful and submit it to T-CDASH. The feedback is handled by the RFS which helps in storing the useful recommendations information along with the corresponding beat and hotspot information in the database. Figure 3.5 depicts the process of displaying recommendations and fetching feedback from police officers in real-time.



Harmspot Identifier: SW21-C

Aggravated Assault	Robbery	Homicide
208.84	108.3	181.84

Recommendations

□ Conduct a vehicle patrol

□ Conduct a foot patrol

□ Other

Figure 3.5: Recommendations and Feedback

3.3 Social Harm Data

As mentioned earlier, CAD, RMS and UCR datasets are made available by the IMPD. CAD and UCR records used in the analysis belong to years 2012, 2013, 2015 and 2016 while the RMS data of 2019 is available for analysis. An input data structure, containing data related to location and time of social harm along with demographic information of the area where the reported incident occurred, is created and fed to the HPPS. HPPS, in turn, generates social harm hotspots. For analyzing the trust framework, CAD, RMS and UCR data are preprocessed and interrelated (described later). Following is a brief description about the structure of CAD, RMS and UCR data.

CAD Data: IMPD’s CAD data consists of various incidents reported to 911 call for service. It has the following schema (see Table 3.2).

Table 3.2: CAD Fields with Description

Field	Description
RUNCODE	A code for each type of incident reported.
DESCRIPT	A brief description about the reported incident.
DISPDATE	Date-time of the reported incident in 24-hour format (YYYY-MM-DD HH:MM:SS format).
IWDISPDATE	Date of the reported incident (YYYYMMDD format).
IWDISPTIME	Time of the reported incident (HHMM format).
LOCATION	Physical address of the reported incident.
XCOOR	X-coordinate of the area of reported incident.
YCOOR	Y-coordinate of the area of reported incident.

RMS Data: A report is generated by the IMPD whenever an incident is investigated. All these reports are stored in IMPD’s RMS. It has the following schema (see Table 3.3).

Table 3.3: RMS Fields with Description

Field	Description
NAT_OFF_CODE	A unique national offence code for each type of recorded incident (Alpha-numeric format).
NAT_OFF_CODE_DESCR	A brief description about the recorded incident.
OFFENSE_DATE	Date-time of the recorded incident in 12-hour format (MM/DD/YYYY HH:MM:SS format).
LATITUDE	Latitude of the area of recorded incident.
LONGITUDE	Longitude of the area of recorded incident.

RMS data is made available through Socrata [44]. Socrata is a Database-as-a-Service (DaaS) platform that helps in managing government data. Table 3.4 provides the schema of the RMS data obtained through Socrata.

Table 3.4: RMS Fields with Description obtained through Socrata

Field	**Description**
incident_id	A unique identifier associated with each recorded incident.
case_number	A unique case number associated with each recorded incident.
incident_datetime	Date and time of the recorded incident (MM/DD/YYYY HH:MM format).
incident_type_primary	Primary incident type of the recorded incident.
incident_description	A brief description about the recorded incident.
address_1	Physical address of the incident.
City	City of the recorded incident.
State	State of the recorded incident.
Latitude	Latitude of the area of recorded incident.
Longitude	Longitude of the area of recorded incident.
created_at	Date and time the incident was recorded (MM/DD/YYYY HH:MM format).
updated_at	Date and time the incident was updated (MM/DD/YYYY HH:MM format).
Location	Geocoordinates of the recorded incident.
hour_of_day	Hour of the day when the incident occurred (24-hour format).
day_of_week	Day of the week when the incident occurred.
parent_incident_type	A generalized incident type, identifying multiple similar incident types, associated with the incident.

UCR Data: Federal Bureau of Investigation (FBI) collects, publishes, archives and maintains social harm records [28]. Most of the analysis on social harm is conducted using this data. It has the following schema (see Table 3.5).

Table 3.5: UCR Fields with Description

Field	**Description**
PARTONE	It identifies the severity of the crime.
CODE	A unique code for each type of recorded incident (Numeric format).
TITLE	A unique text description indicating the type of recorded incident.
DATEOCC	Date of the reported incident (MM/DD/YYYY format).
TIMEOCC	Time of the reported incident (HHMM format format).
LOCATION	Physical address of the reported incident.
XCOOR	X-coordinate of the area of reported incident.
YCOOR	Y-coordinate of the area of reported incident.

3.3.1 Data Preprocessing

As depicted in Tables 3.2 to 3.5, different social harm reporting and management systems store data in different formats, and each has their own schema. To analyze, interrelate, and process these records, it is necessary to convert them in a schema used by the HPPS. To achieve this, each record of CAD, RMS, and UCR is preprocessed so that it can be used with the HPPS.

For CAD, the descriptions entered by 911 officials closely resembled to the type of incident that was reported. Thus, pattern matching was carried out on these event descriptions to map the CAD records into the corresponding HPPS input format. For this, a pattern which closely resembled a given type of incident (e.g., AGG for Aggravated Assault) was chosen and all the records with this pattern in their description (AGG pattern in this example) were mapped to a particular incident code for the HPPS input (Aggravated Assault in this example). With the CAD data set, it is important to note that when a social harm is reported to 911 and recorded in CAD, it is an initial assumption about the harm and the actual harm type is not known until later. Thus, the mappings are based on assumptions that the description is a correct reflection of the actual incident. However, this may not be always true. For example, in 2015, an incident reported as assault in CAD was found to be robbery post investigation.

Table 3.6 indicates the patterns used in the CAD descriptions and the corresponding HPPS input incident mapped – these mappings were carried out in consultation with Dr. Jeremy Carter, Associate Dean for Research, Director of Criminal Justice and Public Safety at IUPUI.

Table 3.6: Mapping CAD Descriptions to CDASH Incidents

CAD Description Pattern	**CDASH Incident Code**
AGG	Aggravated Assault
SHOT	Aggravated Assault
STRUCK	Aggravated Assault
GUN	Aggravated Assault
FIRED	Aggravated Assault
KNIFE	Aggravated Assault
ARSON	Arson
FIRE	Arson
DUI	DWI Arrest
DWI	DWI Arrest
FAKE	Forgery
FORG	Forgery
CARD	Fraud
FRAUD	Fraud
HOMI	Homicide
PURSE	Larceny
SHOPL	Larceny
LARC	Larceny
THEF	Larceny
WALLET	Larceny
VEH	Motor Vehicle Theft
MOLEST	Rape
RAPE	Rape
SEX	Rape
APT	Residential Burglary
BURG	Residential Burglary
RESD	Residential Burglary
RSD	Residential Burglary

Table 3.6 continued

ROBB	Robbery
ASSAL	Simple Assault
ASSAU	Simple Assault
ASSL	Simple Assault
FIGHT	Simple Assault
SUIC	Suicide Attempt
DAM	Vandalism
GRAF	Vandalism
VAND	Vandalism

Similarly, the UCR records are also mapped to the corresponding HPPS input format. Since, UCR data is streamlined, they are mapped to the HPPS inputs using unique UCR codes. Table 3.7 indicates the UCR codes along with the harm title that it represents and the corresponding HPPS input incident.

Table 3.7: Mapping UCR Codes to CDASH Incidents

UCR Code	**UCR Title**	**CDASH Code**
170	AGGRAVATED ASSAULT-GUN	Aggravated Assault
171	AGGRAVATED ASSAULT-KNIFE	Aggravated Assault
172	AGGRAVATED ASSAULT-OTHER WEAPON	Aggravated Assault
173	AGGRAVATED ASSAULT-HANDS,FISTS	Aggravated Assault
329	ARSON-OTHER-CROPS/TIMBR/FENCS/SIGNS	Arson
328	ARSON-OTHR MOBILE,TRAILRS,RECVEH,PLANES	Arson
327	ARSON-MOTOR VEHICLES/CARS/TRUCKS/BUSES	Arson
326	ARSON-ALL OTHER STRUCTURES	Arson
325	ARSON-COMMUNITY/PUBLIC-JAIL,HOSP,SCHOOL	Arson
324	ARSON-OTHR COMMERCIAL,STORE,RESTRNT,OFFICE	Arson
323	ARSON-INDUSTRIAL, MANUFACTURING	Arson

Table 3.7 continued

322	ARSON-STORAGE,GARAGE,BARN,WAREHOUSE	Arson
321	ARSON-OTHR RES,APTS,MOTEL,DORMS,BOARDING	Arson
320	ARSON-SINGLE OCCUPANCY, RESIDENTIAL ETC	Arson
690	DWI ARREST	DWI Arrest
332	FORGERY INVESTIGATION	Forgery
330	FORGERY – CHECK	Forgery
355	FRAUD – WELFARE	Fraud
354	FRAUD – PRESCRIPTION	Fraud
353	FRAUD – OTHER	Fraud
351	FRAUD - CREDIT CARD/ATM	Fraud
350	FRAUD – IMPERSONATION	Fraud
352	FRAUD – CHECK	Fraud
358	FRAUD - BAD CHECK	Fraud
357	FRAUD - IDENTITY THEFT	Fraud
356	FRAUD – WIRE	Fraud
110	CRIMINAL HOMICIDE	Homicide
243	LARCENY- FROM MOTOR VEHICLE	Larceny
256	LARCENY-UNDER 50-FROM BUILDING	Larceny
231	LARCENY-OVER 200-PURSESNATCH	Larceny
232	LARCENY-OVER 200-SHOPLIFTING	Larceny
233	LARCENY-OVER 200-FROM AUTO	Larceny
234	LARCENY-OVER 200-AUTO ACCESSORY	Larceny
235	LARCENY-OVER 200-BICYCLE	Larceny
257	LARCENY-UNDER 50-COIN OPERATED MACH	Larceny
236	LARCENY-OVER 200-FROM BUILDING	Larceny
237	LARCENY-OVER 200-COIN OPERATED MACH	Larceny
238	LARCENY-OVER 200-OTHER	Larceny
240	LARCENY-50 TO 200-POCKETPICKING	Larceny
241	LARCENY-50 TO 200-PURSESNATCH	Larceny
230	LARCENY-OVER 200-POCKETPICKING	Larceny
229	LARCENY-ATTEMPT	Larceny
242	LARCENY-50 TO 200-SHOPLIFTING	Larceny
258	LARCENY-UNDER 50-OTHER	Larceny
360	EMBEZZLEMENT	Larceny
244	LARCENY-50 TO 200-AUTO ACCESSORY	Larceny

Table 3.7 continued

245	LARCENY-50 TO 200-BICYCLE	Larceny
246	LARCENY-50 TO 200-FROM BUILDING	Larceny
247	LARCENY-50 TO 200-COIN OPERATED MACH	Larceny
248	LARCENY-50 TO 200-OTHER	Larceny
250	LARCENY-UNDER 50-POCKETPICKING	Larceny
251	LARCENY-UNDER 50-PURSESNATCH	Larceny
252	LARCENY-UNDER 50-SHOPLIFTING	Larceny
253	LARCENY-UNDER 50-FROM AUTO	Larceny
254	LARCENY-UNDER 50-AUTO ACCESSORY	Larceny
255	LARCENY-UNDER 50-BICYCLE	Larceny
263	RECOVERED VEHICLE STOLEN OJ	Motor Vehicle Theft
260	VEHICLE THEFT	Motor Vehicle Theft
259	ATTEMPT VEHICLE THEFT	Motor Vehicle Theft
122	SEX MISCONDUCT-MINOR	Rape
123	FORCIBLE FONDLING	Rape
120	RAPE	Rape
210	BURG-ATTEMPT-RES NIGHT	Residential Burglary
191	BURG-FORCIBLE ENT-RES DAY	Residential Burglary
201	BURG-NO FORCE-RES DAY	Residential Burglary
200	BURG-NO FORCE-RES NIGHT	Residential Burglary
190	BURG-FORCIBLE ENT-RES NIGHT	Residential Burglary
211	BURG-ATTEMPT-RES DAY	Residential Burglary
140	ROBBERY-ARMED-HIWAY	Robbery
133	ATTEMPT STRONG ARMED ROBBERY	Robbery
132	ATTEMPT ARMED ROBBERY	Robbery
155	ROBBERY-STRONG ARM-BANK	Robbery
154	ROBBERY-STRONG ARM-RESIDENCE	Robbery
153	ROBBERY-STRONG ARM-CHAIN STORE	Robbery
152	ROBBERY-STRONG ARM-OIL STATION	Robbery
151	ROBBERY-STRONG ARM-COMMERCIAL HSE	Robbery
150	ROBBERY-STRONG ARM-HIWAY	Robbery
146	ROBBERY-ARMED-MISCELLANEOUS	Robbery
145	ROBBERY-ARMED-BANK	Robbery
142	ROBBERY-ARMED-OIL STATION	Robbery
143	ROBBERY-ARMED-CHAIN STORE	Robbery
144	ROBBERY-ARMED-RESIDENCE	Robbery
141	ROBBERY-ARMED-COMMERCIAL HOUSE	Robbery
156	ROBBERY-STRONG ARM-MISCELLANEOUS	Robbery
174	ASSAULT-SIMPLE	Simple Assault

Table 3.7 continued

663	SUICIDE ATTEMPT	Suicide Attempt
603	VANDALISM	Vandalism

Lastly, the RMS records maintained by the IMPD are also analyzed and mapped to HPPS inputs. Similar to the UCR data, the RMS data is also streamlined. For RMS, incident descriptions closely resemble the type of incident and are used for generating the mapping. Table 3.8 provides a mapping between various RMS incident descriptions and the corresponding HPPS input incident.

Table 3.8: Mapping RMS Incidents to CDASH Incidents

RMS Incident Descriptions	**CDASH Code**
AGGRAVATED ASSAULT	Aggravated Assault
ALL OTHER LARCENY	Larceny
ARSON	Arson
ARSON INVESTIGATION	Arson
ATTEMPTED BURGLARY	Residential Burglary
ATTEMPTED OR THREATENING SUICIDE	Suicide Attempt
ATTEMPTED ROBBERY	Robbery
BURGLARY IN-PROGRESS	Residential Burglary
BURGLARY INVESTIGATION	Residential Burglary
BURGLARY/BREAKING AND ENTERING	Residential Burglary
COUNTERFEITING/FORGERY	Forgery
CREDIT CARD/AUTOMATIC TELLER MACHINE FRAUD	Fraud
DAMAGE TO PROPERTY	Vandalism
DEATH INVESTIGATION- SUICIDE	Suicide Attempt
DESTRUCTION/DAMAGE/VANDALISM OF PROPERTY	Vandalism
DRIVING UNDER THE INFLUENCE	DWI Arrest
EMBEZZLEMENT	Larceny
FALSE PRETENSES/SWINDLE/CONFIDENCE GAME	Fraud
FIGHT	Simple Assault
FIGHT WITH WEAPON	Aggravated Assault
FIRE INVESTIGATION	Arson
FORCIBLE RAPE	Rape

Table 3.8 continued

FORGERY INVESTIGATION	Forgery
FRAUD INVESTIGATION	Fraud
MOTOR VEHICLE THEFT	Motor Vehicle Theft
MURDER AND NONNEGLIGENT MANSLAUGHTER	Homicide
PERSON ASSAULTED	Simple Assault
PERSON INJURED	Simple Assault
PERSON SHOT	Aggravated Assault
PERSON STABBED	Aggravated Assault
POCKET/PICKING	Larceny
PROPERTY DAMAGE (NON-CRIMINAL EVENT)	Vandalism
PURSE-SNATCHING	Larceny
ROBBERY	Robbery
ROBBERY IN-PROGRESS	Robbery
ROBBERY INVESTIGATION	Robbery
SHOPLIFTING	Larceny
SHOPLIFTING INVESTIGATION	Larceny
SIMPLE ASSAULT	Simple Assault
STOLEN VEHICLE	Motor Vehicle Theft
SUICIDE	Suicide Attempt
SUICIDE- ATTEMPTED	Suicide Attempt
THEFT FROM BUILDING	Larceny
VANDALISM	Vandalism

3.3.2 Data Interrelationship

Trust is an important aspect associated with T-CDASH. As detailed in Section 2.4, to maintain reporter's anonymity and to avoid misuse of reporter's historical reputation, this thesis focused on using Jøsang's opinion model [33] in a similar way as utilized by Ceolin et al. [34]. Through opinion model, a certain degree of trust is assigned to each live incident reported to T-CDASH. This trust is based on three key components that gets associated with the reported event: belief (*b*), disbelief (*d*) and uncertainty (*u*). Section 2.4 presents the mathematical formulae for computing the belief, disbelief and uncertainty. These calculations are based on the number of positive evidences, negative evidences, and total evidences that the system has with respect to the reported live incident. In T-CDASH, to gather these evidences, three key aspects associated with social harm incidents, are taken into consideration.

Location: Geographic coordinates (latitude and longitude) of the location where the reported incident occurred.

Day: Date (day and month) on which the reported incident occurred.

Incident Type: The type of the reported incident.

Based on these three aspects, reported live incident can be interrelated with historical social harm incidents. The interrelated incidents act as evidences for the reported live incident.

For computing the total evidences, two aspects, location and/or day, are considered. With location, we consider a circular range of 110 m (or three decimal places accuracy with respect to latitude and longitude [45]) around the reported incident. All the historical social harm incidents within this range are assumed to contribute towards total evidence. Similarly, historical social harm incidents, which had occurred within a range of days (4 to 7 days) before or after the reported incident's day, in the same month from previous years, also contribute towards the total evidences. These ranges are selected to allow a small buffer with respect to location and day while collecting evidences from the historical data. T-CDASH is made configurable to allow either location or day or both the attributes to contribute towards total evidences.

For positive evidences, the incident type of the incidents that contributed towards the total evidence are considered. All the incidents contributing towards total evidence that have the same incident type as that of the current live incident, act as positive evidences for the live incident.

Thus, interrelating the live incident with historical social harm incidents, we are able to associate certain degree of trust with any live incident.

3.4 Trust Management

Due to the presence of many stakeholders (e.g., community organizations and citizens) in T-CDASH, there is a need to manage the trust associated with their interactions with T-CDASH. Any malicious or incorrect interaction with T-CDASH may affect the hotspot predictions. One way of ensuring and maintaining the accuracy of predictions is to process and filter out live user-inputs (especially from users such as community organizations and citizens) before they are considered for generating hotspots. This processing and filtering stage helps in assigning a trust value to each live interaction – thus, six trust models are created, and their efficacies are compared. These models are:

Ground-truth Model: In this model, all the inputs are assumed to be trustworthy and passed to the HPPS service. No additional processing is done on the inputs. Since, everything is trusted, this model may not perform well while dealing with misleading inputs and filtering them out. Thus, the accuracy of predicting hotspots, obtained via this model, may not be acceptable.

Optimistic Model: The Optimistic model considers a high percentage (80% to 90%) of all the live user-inputs (randomly chosen) to be trustworthy and passes them to the HPPS service. In this model, remaining inputs (10% to 20%) are simply ignored. Since most of the inputs are accepted by this model, it is possible that a high percentage of misleading inputs may contribute towards the hotspot generation. Thus, similar to the Ground-truth Model, this model may also result in incorrect predictions.

Pessimistic Model: It is opposite of the Optimistic model. Here, only a small percentage (10% to 20%) of all the live user-inputs (randomly chosen) are considered to be trustworthy and passed on to the HPPS service. Remaining inputs (80% to 90%) are simply ignored. Since most of the user inputs are ignored, it is safe to assume that most of the misleading inputs will be filtered out from the prediction process. However, as only a smaller percentage of inputs are considered in the prediction process, it is also possible that many genuine inputs are ignored. This may negatively impact the accuracy of hotspots generated by this model.

Average Model: In this model, half of all the live user-inputs (randomly chosen) are considered as trustworthy and passed on to the HPPS service. The remaining half are ignored. Since half of the inputs are randomly chosen and ignored, this model may serve better with considering genuine inputs while ignoring misleading ones as compared to the Optimistic and Pessimistic models. However, since processing is random, accuracy of the system would still be questionable.

Random Model: In this model, a set of live user-inputs are randomly chosen in the process of hotspots generation; others are ignored. This model presents a baseline scenario and can be used in situations when historical data is not available to train HPPS. Again, like the average model, the processing is random and thus, the prediction accuracy would remain indeterminate.

Opinion-based Model: In all the above models, none of the event attributes are taken into consideration while selecting or ignoring the live user-inputs. The Opinion-based model selects or rejects the live inputs based on the trust tuple made up of belief (*b*), disbelief (*d*) and uncertainty (*u*) values. The *b, d* and *u* values are computed in two ways by this model. One method, named Random, randomly assigns values to *b*, *d* and *u* while the other method, named Heuristic, utilizes the interrelation created between live and historical data, as discussed in Section 3.3.2. Since, Random method of this model randomly assigns values, the model accuracy with Random method would be indeterminate. The Heuristic method of this model, however, is based on actual event attributes and its interrelation with historical incidents. Thus, it is expected to perform the best in comparison with all the other models.

3.5 Summary

This chapter has described various processing and interrelationship operations performed on the CAD, RMS and UCR records. The chapter also describes the trust framework with various trust models for associating trust with the social harm events. The following chapter describes and discusses the results obtained by performing various experiments with these trust models with different sets of social harm data.

CHAPTER 4. EXPERIMENTAL RESULTS

This chapter discusses various experiments performed to empirically validate the accuracy of different trust models proposed within the trust framework of T-CDASH to assign a degree of trust with each social harm incident. This thesis uses real-world CAD, RMS and UCR data for experimentation.

4.1 Assumptions

Various experiments are performed on the trust models to analyze their performance. All these experiments are performed under certain assumptions which are as follows:

- All the post investigation social harm records (RMS and UCR records) are assumed to be completely trustworthy.
- The location and date-time recorded for all social harm records in each source (CAD, RMS and UCR) are assumed to correctly reflect the actual location and date-time for the incident.
- It is assumed that the description recorded for an incident reported in CAD is a correct reflection of the actual incident.
- It is also assumed that the conversion of RMS records to UCR records as performed by the law-enforcement agencies is achieved without any errors or misinterpretations.

4.2 Training the Prediction Service

Before comparing the trust models, it is important to train the hotspot prediction service (HPPS). Since the UCR data is highly trustworthy, the HPPS is trained on the UCR data. Also, real-time data is required to test the trust models. Since the CAD data is a real-time reporting of social harm incidents, the CAD records are considered for evaluating the trust models.

A baseline model having accurate predictions is required to compare the performance of trust models. Accurate predictions are generated using completely trustworthy data. This thesis considers the UCR and RMS data to be completely trustworthy. Also, it is necessary to consider all the UCR (available for 2012, 2013, 2015 and 2016) or RMS (available for 2019) records for generating accurate hotspots. Thus, the Ground-truth model is chosen to be the baseline model with the UCR or RMS data. As stated earlier, the CAD records are reported in real-time and prone to errors. Thus, they mimic the live incidents that will be fed to T-CDASH. With this in consideration, the CAD records are fed to models (other than the Ground-truth model) and hotspots generated by them are compared with the hotspots generated by the Ground-truth model. Multiple iterations are performed while comparing the models. Each iteration consists of data belonging to a particular month of the testing period.

4.3 Experiments with Trust Framework

In the experiments performed, the Ground-truth model acts as a baseline model and the accuracy of all the other models (termed as test models) is defined in terms of hotspots matching percentage. The hotspots matching percentage is the percentage of hotspots, generated by a model, that match (have the same location and incident type) with the hotspots generated by the Ground-truth model. Additionally, for all the experiments, two time series data cross validation techniques: Rolling Windows and Rolling Origin are applied to analyze their impact on the accuracy of trust models.

Rolling Windows: Rolling Windows technique considers multiple origins but maintains a fixed training data size by eliminating oldest records in each iteration.

Rolling Origin: Rolling Origin technique considers multiple origins by increasing the training data size in each iteration.

4.3.1 Experiments with 2012 – 2013 Data

This section depicts the results obtained by training the HPPS service on UCR data of 2012-2013 while evaluating the trust models through the CAD and UCR data of 2013.

Optimistic Model: With Optimistic model, three different percentages, 80, 90 and 95, of inputs are considered trustworthy. On an average, the matching percentage was 35.97.

Pessimistic Model: With Pessimistic model, three different percentages, 5, 10 and 20, of inputs are considered trustworthy. On an average, the matching percentage was 48.29.

Average Model: With Average model, it is expected that the hotspots matching percentage will be approximately the average of the matching percentages of the Optimistic and Pessimistic models. In this model, 50 percent of inputs are considered trustworthy. On an average, the matching percentage was 41.10, which is as expected.

Random Model: The Random model is non-deterministic as it randomly considers a set of inputs to be trustworthy. On an average, the matching percentage was 42.23.

The experimental results for the above test models are summarized in Table 4.1.

Table 4.1: Performance of Test Models with 2012-2013 Data

Model	**System**	**Inputs Allowed (%)**	**Hotspots Matched (%)**
Optimistic	Rolling Windows	80	37.46
Optimistic	Rolling Windows	90	36.98
Optimistic	Rolling Windows	95	36.33
Optimistic	Rolling Origin	80	35.60
Optimistic	Rolling Origin	90	34.93
Optimistic	Rolling Origin	95	34.54
Pessimistic	Rolling Windows	5	49.66
Pessimistic	Rolling Windows	10	47.94
Pessimistic	Rolling Windows	20	46.46
Pessimistic	Rolling Origin	5	49.02
Pessimistic	Rolling Origin	10	48.53
Pessimistic	Rolling Origin	20	45.14
Average	Rolling Windows	50	42.93
Average	Rolling Origin	50	39.28
Random	Rolling Windows	Random	42.85
Random	Rolling Origin	Random	41.62

Opinion-based Model: In Opinion-based model, as stated in chapter 3, two methods (Random and Heuristic) are used to assign values to *b*, *d* and *u*. In Random method, if the randomly generated belief value for an incident is above a chosen threshold belief value, the incident is considered for generating hotspots. Similarly, if the randomly generated disbelief value for an incident is above a chosen threshold disbelief value, the incident is ignored. In all other scenarios, the trust on the incident is uncertain and it is either considered or ignored randomly. In Heuristic method, data interrelationship, as detailed in chapter 3 of this thesis, is considered for assigning values to *b*, *d* and *u*. Table 4.2 depicts the percentage of hotspots matched between the hotspots computed by the two methods of Opinion-based model and the Ground-truth model while considering different threshold percentages of belief and disbelief. On an average, the matching percentage of Random method was 40.63 and Heuristic method was 47.59.

Table 4.2: Performance of Opinion-based Model with 2012-2013 Data

Method	**System**	**Is Location Accounted?**	**Is Day Accounted?**	**Belief Threshold (%)**	**Disbelief Threshold (%)**	**Hotspots Matched (%)**
Random	Rolling Windows	No	No	50	50	42.03
Random	Rolling Origin	No	No	50	50	39.24
Heuristic	Rolling Windows	Yes	Yes	50	50	49.47
Heuristic	Rolling Windows	Yes	No	50	50	49.59
Heuristic	Rolling Windows	No	Yes	50	50	48.18
Heuristic	Rolling Windows	Yes	Yes	70	50	47.90
Heuristic	Rolling Windows	Yes	Yes	50	70	46.53
Heuristic	Rolling Windows	Yes	Yes	80	80	46.06
Heuristic	Rolling Windows	Yes	Yes	10	10	46.73
Heuristic	Rolling Windows	Yes	Yes	30	30	49.82
Heuristic	Rolling Origin	Yes	Yes	50	50	48.33

Table 4.2 continued

Heuristic	Rolling Origin	Yes	No	50	50	48.81
Heuristic	Rolling Origin	No	Yes	50	50	47.42
Heuristic	Rolling Origin	Yes	Yes	70	50	46.98
Heuristic	Rolling Origin	Yes	Yes	50	70	45.64
Heuristic	Rolling Origin	Yes	Yes	80	80	45.17
Heuristic	Rolling Origin	Yes	Yes	10	10	45.87
Heuristic	Rolling Origin	Yes	Yes	30	30	49.03

4.3.2 Experiments with 2012, 2013, 2015 and 2016 Data

This section describes the results obtained by training the HPPS service on UCR data from 2012-2013 and 2015-2016 years while evaluating the trust models through the CAD and UCR data of 2015-2016.

Optimistic Model: With Optimistic model, 80 percent of inputs are considered trustworthy.

Pessimistic Model: With Pessimistic model, 20 percent of inputs are considered trustworthy.

Average Model: With Average model, 50 percent of inputs are considered trustworthy.

Random Model: The Random model randomly considers a set of inputs to be trustworthy.

The experimental results for the above models are summarized in Table 4.3.

Table 4.3: Performance of Test Models with 2012, 2013, 2015 and 2016 Data

Model	**System**	**Training Year**	**Testing Year**	**Inputs Allowed (%)**	**Hotspots Matched (%)**
Optimistic	Rolling Windows	2015-2016	2016	80	38.02
Optimistic	Rolling Origin	2015-2016	2016	80	37.59
Optimistic	Rolling Windows	2012-2013	2015	80	23.39
Optimistic	Rolling Origin	2012-2013	2015	80	21.64
Optimistic	Rolling Windows	2012-2013	2016	80	20.41
Optimistic	Rolling Origin	2012-2013	2016	80	19.28
Pessimistic	Rolling Windows	2015-2016	2016	20	48.53
Pessimistic	Rolling Origin	2015-2016	2016	20	49.11
Pessimistic	Rolling Windows	2012-2013	2015	20	25.53
Pessimistic	Rolling Origin	2012-2013	2015	20	23.57
Pessimistic	Rolling Windows	2012-2013	2016	20	26.28
Pessimistic	Rolling Origin	2012-2013	2016	20	26.19
Average	Rolling Windows	2015-2016	2016	50	42.87
Average	Rolling Origin	2015-2016	2016	50	41.45
Average	Rolling Windows	2012-2013	2015	50	25.06
Average	Rolling Origin	2012-2013	2015	50	25.39
Average	Rolling Windows	2012-2013	2016	50	25.81

Table 4.3 continued

Average	Rolling Origin	2012-2013	2016	50	24.86
Random	Rolling Windows	2015-2016	2016	Random	41.86
Random	Rolling Origin	2015-2016	2016	Random	40.93
Random	Rolling Windows	2012-2013	2015	Random	25.16
Random	Rolling Origin	2012-2013	2015	Random	23.72
Random	Rolling Windows	2012-2013	2016	Random	19.85
Random	Rolling Origin	2012-2013	2016	Random	21.94

Opinion-based Model: With both Random and Heuristic methods of the Opinion-based model, the belief and disbelief thresholds are chosen to be at 50 percent. Also, with Heuristic method the location and day parameters are considered while generating evidences. The experimental results for the Opinion-based model is summarized in Table 4.4.

Table 4.4: Performance of Opinion-based Model with 2012, 2013, 2015 and 2016 Data

Method	**System**	**Training Year**	**Testing Year**	**Is Location Accounted?**	**Is Day Accounted ?**	**Belief Threshold (%)**	**Disbelief Threshold (%)**	**Hotspots Matched (%)**
Random	Rolling Windows	2015-2016	2016	No	No	50	50	42.59
Random	Rolling Origin	2015-2016	2016	No	No	50	50	41.64
Random	Rolling Windows	2012-2013	2015	No	No	50	50	24.79
Random	Rolling Origin	2012-2013	2015	No	No	50	50	21.35

Table 4.4 continued

Random	Rolling Windows	2012-2013	2016	No	No	50	50	22.64
Random	Rolling Origin	2012-2013	2016	No	No	50	50	22.06
Heuristic	Rolling Windows	2015-2016	2016	Yes	Yes	50	50	51.73
Heuristic	Rolling Origin	2015-2016	2016	Yes	Yes	50	50	49.28
Heuristic	Rolling Windows	2012-2013	2015	Yes	Yes	50	50	28.59
Heuristic	Rolling Origin	2012-2013	2015	Yes	Yes	50	50	26.43
Heuristic	Rolling Windows	2012-2013	2016	Yes	Yes	50	50	27.58
Heuristic	Rolling Origin	2012-2013	2016	Yes	Yes	50	50	24.93

4.3.3 Experiments with RMS Data

This section details the results obtained by training the HPPS service on the UCR data of 2015-2016 while evaluating the trust models through the RMS data of first five months of 2019. Since, the CAD data for 2019 is not available, simulated CAD data for first five months of 2019 is generated based on the UCR and CAD data of 2016 (most recent CAD and UCR data available). On analyzing the CAD and UCR data of 2016, it is observed that approximately 67% of CAD data is reflected in the UCR records. Based on this, simulated CAD records matching with 67% RMS data is generated. The remaining 33% of CAD records are simulated randomly from UCR records of 2016. For these experiments, the configuration of trust models is same as the configuration used in section 4.2.2. However, it is important to note that since real-world CAD and UCR records are not available for 2019, it is difficult to compare the results with the results obtained from other experiments.

Table 4.5 depicts the performance of Optimistic, Pessimistic, Random and Average Models. Table 4.6 portrays the performance of Opinion-based model.

Table 4.5: Performance of Test Models with RMS Data

Model	**System**	**Inputs Allowed (%)**	**Hotspots Matched (%)**
Optimistic	Rolling Windows	80	48.96
Optimistic	Rolling Origin	80	46.34
Pessimistic	Rolling Windows	20	36.60
Pessimistic	Rolling Origin	20	37.12
Average	Rolling Windows	50	43.58
Average	Rolling Origin	50	42.07
Random	Rolling Windows	Random	46.60
Random	Rolling Origin	Random	43.28

Table 4.6: Performance of Opinion-based Model with RMS Data

Method	**System**	**Is Location Accounted?**	**Is Day Accounted?**	**Belief Threshold (%)**	**Disbelief Threshold (%)**	**Hotspots Matched (%)**
Random	Rolling Windows	No	No	50	50	44.33
Random	Rolling Origin	No	No	50	50	42.83
Heuristic	Rolling Windows	Yes	Yes	50	50	30.66
Heuristic	Rolling Origin	Yes	Yes	50	50	31.47

4.4 Observations and Analyses

4.4.1 Best Model

From Tables 4.1 to 4.4, it can be seen that the Pessimistic model performs best when compared to all the other models. The Pessimistic model is followed by the Opinion-based model with the Heuristic method, the Average model, and lastly the Optimistic model in that order of hotspots matching percentages. Since the performance of the Random model and the Random method of Opinion-based model are indeterminate, it may not be appropriate to compare them directly with other models. However, the matching percentage of the hotspots generated by them are close to that of the Average model. One reason for such hotspot matching behavior is due to the fact that many incidents reported to the CAD are not reported in the UCR in the same way. This is because the incident may have never occurred or after investigation, it was found that some incident other than the actual one was reported. For example, an incident of Simple Assault was reported in CAD. However, during the investigation, it was found that it was a case of Homicide. Another reason is that many incidents are investigated directly by the IMPD without ever being reported in CAD. Thus, CAD and UCR records differ considerably. This justifies the fact that models considering smaller percentages of CAD data for generating hotspots present higher hotspot matching accuracy. These experiments highlight that more the number of inputs ignored, higher is the hotspot match percentage. Accordingly, both the Pessimistic model and the Opinion-based model with the Heuristic method have the highest match percentages. However, it may not be always advisable to ignore a large percentage of inputs. Consider a scenario where a critical live incident is reported. Since both models ignore most of the inputs, even multiple reports by different users reporting the critical incident may get ignored. This may negatively impact the predictions generated by the system. It is also important to note that both the Pessimistic model and the Opinion-based model with the Heuristic method have approximately equal hotspot matching percentages. Since, the Opinion-based model with the Heuristic method takes a more informed decision while considering or ignoring inputs for generating predictions rather than deciding randomly (e.g., the Pessimistic model), it is considered better when compared to the Pessimistic model.

4.4.2 Seasonal Performance of Models

All the experiments are performed on the monthly data of the testing period and then averaged out over the entire year. The hotspots generated for each month are analyzed and compared. A significant observation is that the hotspot match percentage remained close to the average value without displaying any drastic deviations in any month of the year. Thus, a key insight with these experiments is that the performance of various trust models is agnostic from seasonal changes that may occur in social harms occurring in the society.

4.4.3 Effect of Data Cross Validation

As stated earlier, two cross validation techniques for the time series data: Rolling Origin and Rolling Windows are used in the experiments. The difference between the techniques is that the Rolling Origin method considers all the records while generating predictions while the Rolling Windows method eliminates the oldest records. The result of the experiments performed with both techniques are depicted in Tables 4.1 to 4.6. Tashman in [29] indicated that pruning of old records may be unnecessary if the prediction service considers data in a weighted manner, mitigating the influence of any data from distant past. The HPPS service generating hotspots in T-CDASH considers data in a weighted manner. The experiments indicate that the matching percentages remain almost the same no matter which cross validation technique is used. This thesis thus confirms to the observations presented by Tashman in [29].

4.4.4 Effect of Time Intervals between Training and Testing Data

Sections 4.1.1 and 4.2.2 depict experiments involving data from various training and testing years. In particular, the experiments involve four combinations of yearly data for training and testing the trust models as depicted in Table 4.7.

Table 4.7: Training and Testing Years for Evaluating Trust Models

Training Year	**Testing Year**
2012-2013	2013
2015-2016	2016
2012-2013	2015
2012-2013	2016

A key observation from the results obtained while experimenting with the trust models on various years is that, lesser the time interval between the training and testing years data, higher is the hotspots matching accuracy. Considering the Opinion-based model with Heuristic method, the approximate hotspots matching is 50% when training years are 2012-2013 and testing year is 2013 or when training years are 2015-2016 and testing year is 2016. However, the matching percentage drops to approximately 27 when training years are 2012-2013 and testing year is 2015 or when training years are 2012-2013 and testing year is 2016. These results indicate that the CAD and UCR data of consecutive years resemble more closely as compared to when there is a time interval between them. Thus, taking these results into consideration along with the fact that HPPS generates hotspots by considering the social harm events in a weighted manner, assigning more weightage to recent records, it can be said that it is better to train the HPPS on recent data while using the trust models for assigning trust to real-time social harm events.

4.5 Summary

The above sections have discussed the rationale for using the UCR data for training the HPPS and the CAD, RMS and UCR data for evaluating the trust models. Results from different experiments, performed for comparing various models incorporated as part of the trust framework in T-CDASH are detailed. The results indicated that the Opinion-based model with heuristics method proves to be the most optimal model for associating trust with social harm events. All the trust models remained agnostic to seasonal changes in social harms occurring throughout the year. Also, the results obtained from performing data cross validation using Rolling Windows and Rolling Origin techniques proved to be consistent with the observations of Tashman [29].

CHAPTER 5. CONCLUSIONS AND FUTURE WORK

This thesis results in a distributed web application, T-CDASH, that provides a collaborative environment to various stakeholders including the IMPD, community and citizens. T-CDASH predicts location and type of social harm events likely to occur in future. This thesis provides a means for processing and interrelating real-world social harm data from various sources including CAD, RMS and UCR. It also introduces a framework for assigning trust to real-time social harm events reported to T-CDASH. The trust framework includes different trust models each having a unique way of associating trust with the social harm incidents. Various experiments are performed with the trust models for analyzing their performance using social harm data from multiple years. This thesis concludes by indicating the optimal model for assigning trust to real-time social harm events. Following are the contributions of the thesis:

- A distributed web application, T-CDASH, is developed and empirically validated using experiments that are performed on real-world social harm records for mitigating social harm.
- A procedure to process and interrelate 911's call for service data (CAD) and post-investigation data (RMS and UCR) is proposed.
- Trust framework with six trust models: Ground-truth, Optimistic, Pessimistic, Average, Random and Opinion-based model, is created for associating trust with social harm events.
- Opinion-based model with Heuristic method, taking into consideration social harm event attributes while assigning trust, proves to be the most efficient trust model.
- Two time series data cross validation techniques involving Rolling Origin and Rolling Windows are incorporated to analyze its impact on association of trust with social harm events.
- Finally, it can be concluded that all the social harm incidents cannot be randomly trusted. Thus, it is necessary to incorporate a trust framework for associating trust with social harm events.

This thesis can be extended in many possible directions in future. Additional trust models that take into consideration other aspects associated with social harm incidents such as the number of times an incident is reported, and the incident severity can be incorporated while estimating an incident's trustworthiness. In terms of model comparison metrics, other techniques such as Earth Movers Distance [46] can be incorporated for measuring the hotspot matching accuracy of the models.

LIST OF REFERENCES

[1] Lasslett, K. (2010). Crime or social harm? A dialectical perspective. Crime, Law and Social Change, 54(1), 1-19.

[2] Pemberton, S. (2007). Social harm future (s): exploring the potential of the social harm approach. Crime, Law and Social Change, 48(1-2), 27-41.

[3] Hillyard, P., & Tombs, S. (2007). From 'crime' to social harm?. Crime, law and social change, 48(1-2), 9-25.

[4] Greene, J. R. (2014). New directions in policing: Balancing prediction and meaning in police research. Justice quarterly, 31(2), 193-228.

[5] Mohler, G., Carter, J., & Raje, R. (2018). Improving social harm indices with a modulated Hawkes process. International Journal of Forecasting, 34(3), 431-439.

[6] Weisburd, D., & Eck, J. E. (2004). What can police do to reduce crime, disorder, and fear?. The Annals of the American Academy of Political and Social Science, 593(1), 42-65.

[7] Rossmo, D. K. (1999). Geographic profiling. CRC press.

[8] McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. Machine Learning and Applications: An International Journal (MLAIJ), 2(1), 1-12.

[9] Kiani, R., Mahdavi, S., & Keshavarzi, A. (2015). Analysis and prediction of crimes by clustering and classification. International Journal of Advanced Research in Artificial Intelligence, 4(8), 11-17.

[10] Wang, B., Zhang, D., Zhang, D., Brantingham, P. J., & Bertozzi, A. L. (2017). Deep learning for real time crime forecasting. arXiv preprint arXiv:1707.03340.

[11] Greene, J. R. (2014). New directions in policing: Balancing prediction and meaning in police research. Justice quarterly, 31(2), 193-228.

[12] Ratcliffe, J. H. (2015). Towards an index for harm-focused policing. Policing: A Journal of Policy and Practice, 9(2), 164-182.

[13] Kelling, G. L., & Moore, M. H. (1989). The evolving strategy of policing. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.

[14] Wakefield, A. (2007). Continuing the Discussion on Community Policing, Issue 2 Carry on Constable? Revaluing Foot Patrol. Policing: A journal of Policy and Practice, 1(3), 342-355.

[15] Ratcliffe, J. H., Taniguchi, T., Groff, E. R., & Wood, J. D. (2011). The Philadelphia foot patrol experiment: A randomized controlled trial of police patrol effectiveness in violent crime hotspots. Criminology, 49(3), 795-831.

[16] Groff, E. R., Ratcliffe, J. H., Haberman, C. P., Sorg, E. T., Joyce, N. M., & Taylor, R. B. (2015). Does what police do at hot spots matter? The Philadelphia policing tactics experiment. Criminology, 53(1), 23-53.

[17] Kelling, G. L., Pate, A., Ferrara, A., Utne, M., & Brown, C. E. (1981). The Newark foot patrol experiment. Washington, DC: Police Foundation, 94-96.

[18] Kelling, G. L., Pate, T., Dieckman, D., & Brown, C. (1974). The Kansas City Preventive Patrol Experiment: A Tecnical Report. Washington, DC: Police Foundation.

[19] Pate, A. M. (1986). Experimenting with foot patrol: The Newark experience. Community crime prevention: Does it work, 137-156.

[20] Wilson, J. Q., & Boland, B. (1977). The effect of the police on crime. LAW & Soc'y REv., 12, 367.

[21] Sampson, R. J., & Cohen, J. (1988). Deterrent effects of the police on crime: A replication and theoretical extension. Law & Soc'y Rev., 22, 163.

[22] Kubrin, C. E., Messner, S. F., Deane, G., McGeever, K., & Stucky, T. D. (2010). Proactive policing and robbery rates across US cities. Criminology, 48(1), 57-97.

[23] Sherman, L. W., Shaw, J. W., & Rogan, D. P. (1995). The Kansas City Gun Experiment. Population, 4, 8-142.

[24] McGarrell, E. F., Chermak, S., & Weiss, A. (2002). Reducing gun violence: Evaluation of the Indianapolis Police Department's directed patrol project series: Special report. Washington, DC: National Institute of Justice.

[25] Koper, C. S., & Mayo-Wilson, E. (2006). Police crackdowns on illegal gun carrying: A systematic review of their impact on gun crime. Journal of experimental criminology, 2(2), 227-261.

[26] Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf

[27] Standard Functional Specifications for Law Enforcement Records Management Systems (RMS) https://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf

[28] Uniform Crime Reporting https://www.fbi.gov/services/cjis/ucr

[29] Tashman, L. J. (2000). Out-of-sample tests of forecasting accuracy: an analysis and review. International journal of forecasting, 16(4), 437-450.

[30] Bogomolov, A., Lepri, B., Staiano, J., Oliver, N., Pianesi, F., & Pentland, A. (2014, November). Once upon a crime: towards crime prediction from demographics and mobile data. In Proceedings of the 16th international conference on multimodal interaction (pp. 427-434). ACM.

[31] Yu, C. H., Ding, W., Chen, P., & Morabito, M. (2014, May). Crime forecasting using spatio-temporal pattern with ensemble learning. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 174-185). Springer, Cham.

[32] Chen, X., Cho, Y., & Jang, S. Y. (2015, April). Crime prediction using Twitter sentiment and weather. In 2015 Systems and Information Engineering Design Symposium (pp. 63-68). IEEE.

[33] Jøsang, A. (1997, December). Artificial reasoning with subjective logic. In Proceedings of the second Australian workshop on commonsense reasoning (Vol. 48, p. 34). Perth:[sn].

[34] Ceolin, D., Groth, P. T., & Van Hage, W. R. (2010). Calculating the Trust of Event Descriptions using Provenance. In SWPM@ ISWC.

[35] Reputation Systems https://en.wikipedia.org/wiki/Reputation_system

[36] Furtado, V., Ayres, L., De Oliveira, M., Vasconcelos, E., Caminha, C., D'Orleans, J., & Belchior, M. (2010). Collective intelligence in law enforcement–The WikiCrimes system. Information Sciences, 180(1), 4-17.

[37] Pandey, S., Chowdhury, N., Patil, M., Raje, R. R., Shreyas, C. S., Mohler, G., & Carter, J. (2018, September). CDASH: Community Data Analytics for Social Harm Prevention. In 2018 IEEE International Smart Cities Conference (ISC2) (pp. 1-8). IEEE.

[38] Apache Kafka https://kafka.apache.org

[39] Keyhole Markup Language https://en.wikipedia.org/wiki/Keyhole_Markup_Language

[40] GeoJSON https://en.wikipedia.org/wiki/GeoJSON

[41] Shapefile https://en.wikipedia.org/wiki/Shapefile

[42] Geographic Information System file format https://en.wikipedia.org/wiki/GIS_file_formats

[43] ArcGIS https://www.arcgis.com/index.html

[44] Socrata https://moto.data.socrata.com/dataset/Indianapolis-Metropolitan-Police-Department/n3wc-t646

[45] Latitude and Longitude Precision https://gizmodo.com/how-precise-is-one-degree-of-longitude-or-latitude-1631241162

[46] Earth Movers Distance http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/RUBNER/emd.htm

PUBLICATION

Pandey, Saurabh, et al. "CDASH: Community Data Analytics for Social Harm Prevention." 2018 IEEE International Smart Cities Conference (ISC2). IEEE, 2018.