Data Mining And Homeland Security An Overview Epic

Data Warehousing and Mining (DWM) is the science of managing and analyzing large datasets and discovering novel patterns and in recent years has emerged as a particularly exciting and industrially relevant area of research. Prodigious amounts of data are now being generated in domains as diverse as market research, functional genomics and pharmaceuticals; intelligently analyzing these data, with the aim of answering crucial questions and helping make informed decisions, is the challenge that lies ahead. The Encyclopedia of Data Warehousing and Mining provides a comprehensive, critical and descriptive examination of concepts, issues, trends, and challenges in this rapidly expanding field of data warehousing and mining (DWM). This encyclopedia consists of more than 350 contributors from 32 countries, 1,800 terms and definitions, and more than 4,400 references. This authoritative publication offers in-depth coverage of evolutions, theories, methodologies, functionalities, and applications of DWM in such interdisciplinary industries as healthcare informatics, artificial intelligence, financial modeling, and applied statistics, making it a single source of knowledge and latest discoveries in the field of DWM.

Highlights of GAO-05-866, a report to the Ranking Minority Member, Subcommittee on Oversight of Government Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate The federal government's increased use of data mining since the terrorist attacks of September 11, 2001, has raised public and congressional concerns. As a result, GAO was asked to describe the characteristics of five federal data mining efforts and to determine whether agencies are providing adequate privacy and security protection for the information systems used in the efforts and for individuals potentially affected by these data mining efforts.

Advances in hardware technology have increased the capability to store and record personal data. This has caused concerns that personal data may be abused. This book proposes a number of techniques to perform the data mining tasks in a privacy-preserving way. This edited volume contains surveys by distinguished researchers in the privacy field. Each survey includes the key research content as well as future research directions of a particular topic in privacy. The book is designed for researchers, professors, and advanced-level students in computer science, but is also suitable for practitioners in industry.

The Mathematical Sciences' Role in Homeland Security

Balancing Privacy & Security: The Privacy Implications of Government Data Mining Programs: Congressional Hearing

Encyclopedia of Data Warehousing and Mining

Practical Data Mining

Survey of DHS Data Mining Activities

Intelligence and Security Informatics for International Security

This book is nothing less than a complete and comprehensive survey of the state-of-the-art of terrorism informatics. It covers the application of advanced methodologies and information fusion and analysis. It also lays out techniques to acquire, integrate, process, analyze, and manage the diversity of terrorism-related information for international and homeland security-related applications. The book details three major areas of terrorism research: prevention, detection, and established governmental responses to terrorism. It systematically examines the current and ongoing research, including recent case studies and application of terrorism informatics techniques. The coverage then presents the critical and relevant social/technical areas to terrorism research including social, privacy, data confidentiality, and legal challenges.

In 2004, the Government Accountability Office provided a report detailing approximately 200 government-based data-mining projects. While there is comfort in knowing that there are many effective systems, that comfort isn't worth much unless we can determine that these systems are being effectively and responsibly employed. Written by one of the most respected consultants in the area of data mining and security, Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies reviews the tangible results produced by these systems and evaluates their effectiveness. While CSI-type shows may depict information sharing and analysis that are accomplished with the push of a button, this sort of proficiency is more fiction than reality. Going beyond a discussion of the various technologies, the author outlines the issues of information sharing and the effective interpretation of results, which are critical to any integrated homeland security effort. Organized into three main sections, the book fully examines and outlines the future of this field with an insider's perspective and a visionary's insight. Section 1 provides a fundamental understanding of the types of data that can be used in current systems. It covers approaches to analyzing data and clearly delineates how to connect the dots among different data elements Section 2 provides real-world examples derived from actual operational systems to show how data is used, manipulated, and interpreted in domains involving human smuggling, money laundering, narcotics trafficking, and corporate fraud Section 3 provides an overview of the many information-sharing systems, organizations, and task forces as well as data interchange formats. It also discusses optimal information-sharing and analytical architectures Currently, there is very little published literature that truly defines real-world systems. Although politics and other factors all play into how much one agency is willing to support the sharing of its resources, many now embrace the wisdom of that path. This book will provide those individuals with an understanding of what approaches are currently available and how they can be most effectively employed.

This new Handbook addresses the state of the art in the application of operations research models to problems in preventing terrorist attacks, planning and preparing for emergencies, and responding to and recovering from disasters. The purpose of the book is to enlighten policy makers and decision makers about the power of operations research to help organizations plan for and respond to terrorist attacks, natural disasters, and public health emergencies, while at the same time providing researchers with one single source of up-to-date research and applications. The Handbook consists of nine separate chapters: Using Operations Research Methods for Homeland Security Problems Operations Research and Homeland Security: Overview and Case Study of Pandemic Influenza Deployed Security Games for Patrol Planning Interdiction Models and Applications Time Discrepant Shipments in Manifest Data Achieving Realistic Levels of Defensive Hedging Mitigating the Risk of an Anthrax Attack with Medical Countermeasures Service Networks for Public Health Preparedness and Large-scale Disaster Relief Efforts Disaster Response Planning in the Private Sector

Department of Homeland Security Appropriations For 2008, Part 5, February 15, 2007, 110-1 Hearings, *

How Data Mining Threatens Student Privacy

Knowledge Management and Data Mining for Homeland Security

Terrorism Informatics

From Sensing and Encrypting to Mining and Modeling

A Framework for Program Assessment

All U.S. agencies with counterterrorism programs that collect or "mine" personal data -- such as phone records or Web sites visited -- should be required to evaluate the programs' effectiveness, lawfulness, and impacts on privacy. A framework is offered that agencies can use to evaluate such information-based programs, both classified and unclassified. The book urges Congress to re-examine existing privacy law to assess how privacy can be protected in current and future programs and recommends that any individuals harmed by violations of privacy be given a meaningful form of redress. Two specific technologies are examined: data mining and behavioral surveillance. Regarding data mining, the book concludes that although these methods have been useful in the private sector for spotting consumer fraud, they are less helpful for counterterrorism because so little is known about what patterns indicate terrorist activity. Regarding behavioral surveillance in a counterterrorist context, the book concludes that although research and development on certain aspects of this topic are warranted, there is no scientific consensus on whether these techniques are ready for operational use at all in counterterrorism.

Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis, 2nd Edition, describes clearly and simply how crime clusters and other intelligence can be used to deploy security resources most effectively. Rather than being reactive, security agencies can anticipate and prevent crime through the appropriate application of data mining and the use of standard computer programs. Data Mining and Predictive Analysis offers a clear, practical starting point for professionals who need to use data mining in homeland security, security analysis, and operational law enforcement settings. This revised text highlights new and emerging technology, discusses the importance of analytic context for ensuring successful implementation of advanced analytics in the operational setting, and covers new analytic service delivery models that increase ease of use and access to high-end technology and analytic capabilities. The use of predictive analytics in intelligence and security analysis enables the development of meaningful, information based tactics, strategy, and policy decisions in the operational public safety and security environment. Discusses new and emerging technologies and techniques, including up-to-date information on predictive policing, a key capability in law enforcement and security Demonstrates the importance of analytic context beyond software Covers new models for effective delivery of advanced analytics to the operational environment, which have increased access to even the most powerful capabilities Includes terminology, concepts, practical application of these concepts, and examples to highlight specific techniques and approaches in crime and intelligence analysis

*Investigative Data Mining for Security and Criminal Detection is the first book to outline how data mining technologies can be used to combat crime in the 21st century. It introduces security managers, law enforcement investigators, counter-intelligence agents, fraud specialists, and information security analysts to the latest data mining techniques and shows how they can be used as investigative tools. Readers will learn how to search public and private databases and networks to flag potential security threats and root out criminal activities even before they occur. The groundbreaking book reviews the latest data mining technologies including intelligent agents, link analysis, text mining, decision trees, self-organizing maps, machine learning, and neural networks. Using clear, understandable language, it explains the application of these technologies in such areas as computer and network security, fraud prevention, law enforcement, and national defense. International case studies throughout the book further illustrate how these technologies can be used to aid in crime prevention. Investigative Data Mining for Security and Criminal Detection will also serve as an indispensable resource for software developers and vendors as they design new products for the law enforcement and intelligence communities. Key Features: * Covers cutting-edge data mining technologies available to use in evidence gathering and collection * Includes numerous case studies, diagrams, and screen captures to illustrate real-world applications of data mining * Easy-to-read format illustrates current and future data mining uses in preventative law enforcement, criminal profiling, counter-terrorist initiatives, and forensic science * Introduces cutting-edge technologies in evidence gathering and collection, using clear non-technical language * Illustrates current and future applications of data mining tools in preventative law enforcement, homeland security, and other areas of crime detection and prevention * Shows how to construct predictive models for detecting criminal activity and for behavioral profiling of perpetrators * Features numerous Web links, vendor resources, case studies, and screen captures illustrating the use of artificial intelligence (AI) technologies*

Sports Data Mining

Joint Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives and the Subcommittee on Early Childhoo

Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative

A Case for Data Mining and Information Assurance to Enhance Homeland Security

Crs Report for Congress

Balancing Privacy and Security

There are more than one billion documents on the Web, with the count continually rising at a pace of over one million new documents per day. As information increases, the motivation and interest in data warehousing and mining research and practice remains high in organizational interest. The Encyclopedia of Data Warehousing and Mining, Second Edition, offers thorough exposure to the issues of importance in the rapidly changing field of data warehousing and mining. This essential reference source informs decision makers, problem solvers, and data mining specialists in business, academia, government, and other settings with over 300 entries on theories, methodologies, functionalities, and applications.

How data mining threatens student privacy : joint hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives and the Subcommittee on Early Childhood, Elementary, and Secondary Education of the Committee on Education and the Workforce, House of Representatives, One Hundred Thirteenth Co

This practical book offers you expert guidance on sensors and the preprocessing of sensed data, the handling of sensed data with secure and safe procedures, and the design, modeling and simulation of complex HS systems. You learn how to store, encrypt and mine sensitive data. Further, the book shows how data is transmitted and received along wired or wireless networks, operating on electromagnetic channels.

Reengineering the Immigration System

An Overview

Intelligent Data Analytics for Terror Threat Prediction

Privacy-Preserving Data Mining

Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred Eleventh Congress, First Session

Department of Homeland Security Appropriations For 2007, Part 5, February 16, 2006, 109-2 Hearing, *

Data mining is emerging as one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. This report discusses the data mining uses (i.e. Terrorism Information Awareness (TIA) Program) and issues (i.e. data quality, interoperability, privacy), as well as the limitations of data mining.

Used by corporations, industry, and government to inform and fuel everything from focused advertising to homeland security, data mining can be a very useful tool across a wide range of applications. Unfortunately, most books on the subject are designed for the computer scientist and statistical illuminati and leave the reader largely adrift in tech

The IEEE International Conference on Intelligence and Security Informatics (ISI) and Pacific Asia Workshop on Intelligence and Security Informatics (PAISI) conference series (http://www. isiconference. org) have drawn significant attention in the recent years. Intelligence and Security Informatics is concerned with the study of the dev- opment and use of advanced information technologies and systems for national, int- national, and societal security-related applications. The ISI conference series have brought together academic researchers, law enforcement and intelligence experts, - formation technology consultant and practitioners to discuss their research and pr- tice related to various ISI topics including ISI data management, data and text mining for ISI applications, terrorism informatics, deception and intent detection, terrorist and criminal social network analysis, public health and bio-security, crime analysis, - ber-infrastructure protection, transportation infrastructure security, policy studies and evaluation, information assurance, among others. In this book, we collect the work of the most active researchers in the area. Topics include data and text mining in terr- ism, information sharing, social network analysis, Web-based intelligence monitoring and analysis, crime data analysis, infrastructure protection, deception and intent det- tion and more. Scope and Organization The book is organized in four major areas. The first unit focuses on the terrorism - formatics and data mining. The second unit discusses the intelligence and crime analysis. The third unit covers access control, infrastructure protection, and privacy. The forth unit presents surveillance and emergency response.

How Data Mining Threatens Student Privacy :.

The Privacy Implications of Government Data Mining Programs : Hearing Before the Committee on the Judiciary, United States Senate, One Hundred Tenth Congress, First Session, January 10, 2007

DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism

Early Attention to Privacy in Developing a Key Dhs Program Could Reduce Risks

Information Sharing and Data Mining

Models and Algorithms

Data mining -- a technique for extracting useful information from large volumes of data -- is one type of analysis that the Department of Homeland Security (DHS) uses to help detect and prevent terrorist threats. While data-mining systems offer a number of promising benefits, their use also raises privacy concerns. This report: (1) assesses DHS policies for evaluating the effectiveness and privacy protections of data-mining systems used for counterterrorism; (2) assesses DHS agencies' efforts to evaluate the effectiveness and privacy protections of their data-mining systems; and (3) describes the challenges facing DHS in implementing an effective evaluation framework. Includes recommendations. Charts and tables. A print on demand report.

The government's interest in using technology to detect terrorism and other threats has led to increased use of data mining. A technique for extracting useful information from large volumes of data, data mining offers potential benefits but also raises privacy concerns when the data include personal information. GAO was asked to review the development by the Department of Homeland Security (DHS) of a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement). Specifically, GAO was asked to determine (1) the tool's planned capabilities, uses, and associated benefits and (2) whether potential privacy issues could arise from using it to process personal information and how DHS has addressed any such issues. GAO reviewed program documentation and discussed these issues with DHS officials.

Increasingly, crimes and fraud are digital in nature, occurring at breakneck speed and encompassing large volumes of data. To combat this unlawful activity, knowledge about the use of machine learning technology and software is critical. Machine Learning Forensics for Law Enforcement, Security, and Intelligence integrates an assortment of deductive

Intelligence Gathering and Crime Analysis

Homeland Security Technology Challenges

Investigative Data Mining for Security and Criminal Detection

Handbook of Operations Research for Homeland Security

Department of Homeland Security Appropriations for 2010

An Overview of Issues and Challenges Facing the Department of Homeland Security

Data mining has become one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. In the context of homeland security, data mining can be a potential means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records. While data mining represents a significant advance in the type of analytical tools currently available, there are limitations to its capability. One limitation is that although data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns. These types of determinations must be made by the user. A second limitation is that while data mining can identify connections between behaviors and/or variables, it does not necessarily identify a causal relationship. Successful data mining still requires skilled technical and analytical specialists who can structure the analysis and interpret the output. Data mining is becoming increasingly common in both the private and public sectors. Industries such ...

Data mining has become one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. In the context of homeland security, data mining can be a potential means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records. While data mining represents a significant advance in the type of analytical tools currently available, there are limitations to its capability. One limitation is that although data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns. These types of determinations must be made by the user. A second limitation is that while data mining can identify connections between behaviors and/or variables, it does not necessarily identify a causal relationship. Successful data mining still requires skilled technical and analytical specialists who can structure the analysis and interpret the output. Data mining is becoming increasingly common in both the private and public sectors. As with other aspects of data mining, while technological capabilities are important, there are other implementation and oversight issues that can influence the success of a project's outcome. One issue is data quality. A second issue is the interoperability of the data mining software and databases being

used by different agencies. A third issue is mission creep, or the use of data for purposes other than for which the data were originally collected. A fourth issue is privacy. It is anticipated that congressional oversight of data mining projects will grow as data mining efforts continue to evolve.

Data mining is the process of extracting hidden patterns from data, and it's commonly used in business, bioinformatics, counter-terrorism, and, increasingly, in professional sports. First popularized in Michael Lewis' best-selling Moneyball: The Art of Winning An Unfair Game, it is has become an intrinsic part of all professional sports the world over, from baseball to cricket to soccer. While an industry has developed based on statistical analysis services for any given sport, or even for betting behavior analysis on these sports, no research-level book has considered the subject in any detail until now. Sports Data Mining brings together in one place the state of the art as it concerns an international array of sports: baseball, football, basketball, soccer, greyhound racing are all covered, and the authors (including Hsinchun Chen, one of the most esteemed and well-known experts in data mining in the world) present the latest research, developments, software available, and applications for each sport. They even examine the hidden patterns in gaming and wagering, along with the most common systems for wager analysis.

Department of Homeland Security Appropriations for 2009, Part 2, February 13, 2008, 110-2 Hearings, *

Data Mining for Intelligence, Fraud & Criminal Detection

Advanced Analytics & Information Sharing Technologies

Techniques and Applications

Encyclopedia of Data Warehousing and Mining, Second Edition

Background and Issues for Congress

Data mining is emerging as one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. In the context of homeland security, data mining is often viewed as a potential means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records. While data mining represents a significant advance in the type of analytical tools currently available, there are limitations to its capability. One limitation is that although data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns. These types of determinations must be made by the user. A second limitation is that while data mining can identify connections between behaviors and/or variables, it does not necessarily identify a causal relationship. To be successful, data mining still requires skilled technical and analytical specialists who can structure the analysis and interpret the output that is created. Data mining is becoming increasingly common in ...

Reflects a decade of leading-edge research on intelligence and security informatics. Dr Chen is researcher at the Artificial Intelligence Laboratory and the NSF COPLINK Center for Homeland Security Information Technology Research. Describes real-world community situations. Targets wide-ranging audience: from researchers in computer science, information management and information science via analysts and policy makers in federal departments and national laboratories to consultants in IT hardware, communication, and software companies.

Intelligent data analytics for terror threat prediction is an emerging field of research at the intersection of information science and computer science, bringing with it a new era of tremendous opportunities and challenges due to plenty of easily available criminal data for further analysis. This book provides innovative insights that will help obtain interventions to undertake emerging dynamic scenarios of criminal activities. Furthermore, it presents emerging issues, challenges and management strategies in public safety and crime control development across various domains. The book will play a vital role in improvising human life to a great extent. Researchers and practitioners working in the fields of data mining, machine learning and artificial intelligence will greatly benefit from this book, which will be a good addition to the state-of-the-art approaches collected for intelligent data analytics. It will also be very beneficial for those who are new to the field and need to quickly become acquainted with the best performing methods. With this book they will be able to compare different approaches and carry forward their research in the most important areas of this field, which has a direct impact on the betterment of human life by maintaining the security of our society. No other book is currently on the market which provides such a good collection of state-of-the-art methods for intelligent data analytics-based models for terror threat prediction, as intelligent data analytics is a newly emerging field and research in data mining and machine learning is still in the early stage of development.

Intelligence and Security Informatics

Data Mining

Architectures, Methodologies, Techniques, and Applications

Data Mining Report to Congress

Data Mining and Predictive Analysis

Machine Learning Forensics for Law Enforcement, Security, and Intelligence

The Department of Homeland Security (DHS) Privacy Office (DHS Privacy Office or Office) is providing this report to Congress pursuant to Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), entitled the Federal Agency Data Mining Reporting Act of 2007 (Data Mining Reporting Act or the Act). This report discusses activities currently deployed or under development in the Department that meet the Data Mining Reporting Act's definition of data mining, and provides the information set out in the Act's reporting requirements for data mining activities. In the 2011 DHS Data Mining Report, the DHS Privacy Office discussed the following Department programs that engage in data mining, as defined by the Data Mining Reporting Act: (1) The Automated Targeting System (ATS), which is administered by U.S. Customs and Border Protection (CBP) and includes modules for inbound (ATS-N) and outbound (ATS-AT) cargo, land border crossings (ATS-L), and passengers (ATS-P); and (2) The Data Analysis and Research for Trade Transparency System (DARTTS), which is administered by U.S. Immigration and Customs Enforcement (ICE). This year's report, covering the period December 2011 through December 2012, presents the complete descriptions of ATS-N, ATS-AT, ATS-L, ATS-P, and DARTTS provided in the 2011 DHS Data Mining Report, with updates on modifications, additions, and other developments that have occurred in the current reporting year, including use of ATS by DHS components other than CBP. In addition, the DHS Privacy Office has identified two new uses of ATS that are discussed below: the vetting of non-immigrant and immigrant visa applications in ATS-P for the U.S. Department of State; and the United States Coast Guard's Interagency Operations Center ATS-Enhanced Watchkeeper System. The 2011 Report included a brief summary of CBP's Analytical Framework for Intelligence (AFI), which was then in development. This year's report includes a detailed description of AFI as an operational system. Additional information on DARTTS and on the Transportation Security Administration's (TSA) Secure Flight Program's use of ATS is being provided separately to Congress in two annexes to this report that contain Law Enforcement Sensitive Information and Sensitive Security Information, respectively. The Homeland Security Act of 2002, as amended (Homeland Security Act), expressly authorizes the Department to use data mining, among other analytical tools, in furtherance of its mission. DHS exercises its authority to engage in data mining in the programs discussed in this report, all of which the DHS Chief Privacy Officer has reviewed for potential impact on privacy. The Chief Privacy Officer's authority for reviewing DHS data mining activities stems from three principal sources: the Privacy Act of 1974, as amended (Privacy Act); the E-Government Act of 2002 (E-Government Act); and Section 222 of the Homeland Security Act, which states that the Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information."

This is a print on demand edition of a hard to find publication. The 9/11 Commission cited breakdowns in info. sharing and the failure to fuse pertinent intelligence as key factors in the failure to prevent the 9/11 attacks. Suspicious Activity Reports (SARs) contain info. about criminal activity that may also reveal terrorist pre-operational planning. The Nationwide SAR Initiative (NSI) is an effort to have fed., state, local, and tribal law enforcement org. participate in a standardized, integrated approach to gathering, documenting, processing, and analyzing terrorism-related SARs. This report describes the NSI, the rationale for the sharing of terrorism-related SARs, and how the NSI seeks to achieve this objective. It examines the privacy and civil liberties concerns raised by the initiative. Charts and tables.

Mathematical sciences play a key role in many important areas of Homeland Security including data mining and image analysis and voice recognition for intelligence analysis, encryption and decryption for intelligence gathering and computer security, detection and epidemiology of bioterriost attacks to determine their scope, and data fusion to analyze information coming from simultaneously from several sources. This report presents the results of a workshop focusing on mathematical methods and techniques for addressing these areas. The goal of the workshop is to help mathematical scientists and policy makers understand the connections between mathematical sciences research and these homeland security applications.

Proceedings of a Workshop

Protecting Individual Privacy in the Struggle Against Terrorists

2007 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties

Full Hearing of the Committee on Homeland Security, House of Representatives, One Hundred Tenth Congress, First Session, February 7, 2007

Data Mining and Homeland Security