On U.S. Homeland Security and Database Technology

Won Kim, Cyber Database Solutions, USA

ABSTRACT

Since the terrorist attacks of September 11, 2001, “homeland security” has become the centerpiece of U.S. domestic and foreign policies. The number of terrorists is a tiny fraction of all the people who live in or enter the U.S. However, given the enormous consequences of a repeat of the September 11 attacks, all non-terrorists have been subjected to security measures. The cost of all the security measures includes not only the cost of human resources, deployment of defensive weaponry and technology purchases, but also the time that all people waste. One of the ways to reduce costs is to make terrorist-related intelligence more precise and accurate, so that efforts to track, arrest and deter terrorists, their supporters and movements of funds and weapons can be more precisely directed. One of the ways to make such intelligence more precise is the use of data gathered and stored in databases, and database and related technologies to query, search and mine the databases. This paper first reviews the difficulties in tracking terrorist suspects and their activities. It then examines how databases, and database and related technologies, can be used and made more effective in aiding the war against terror.

Keywords: data integration; data quality; data warehousing; database systems; homeland security; metadata management; terrorism

INTRODUCTION

In his 1994 novel “Debt of Honor,” Tom Clancy describes the near total annihilation of all three branches of the U.S. government by a pilot who plunges a commercial airliner onto the Capitol building during the State of the Union speech by a U.S. President. On September 11, 2001, Al Qaeda terrorists plunged commercial airliners into the twin towers of the World Trade Center, and onto a wing of the Pentagon. The U.S. government then declared war against terror, and has taken numerous actions and measures to prevent a repeat of similar attacks in the U.S. and against U.S. interests outside the U.S. The U.S. launched wars against Afghanistan and Iraq. Congress passed the Patriots Act to make it easier for the U.S. government to monitor and arrest terrorist suspects. The U.S. created a mammoth Department of Homeland Security to consolidate many of the government agencies that perform func-
tions related to “U.S. homeland security” (to be referred to as “homeland security” henceforth), such as immigration, customs, border control, transportation safety, and so forth. The Department has introduced various security measures for air travel safety. It created a national terror alert indication system to make people aware of the overall level of security threats. Different alert levels activate different sets of procedures and security resources over different sets of potential targets of attack. The Department of Defense will soon require thousands of contractors to attach radio frequency identification (RFID) tags on cases and pallets of items (e.g. chemical and biological warfare suits) they will deliver to the Department in order to better keep track of the items.

The Difficulties

Despite the determined and massive efforts by the U.S. government, it is clear that it simply is impossible to prevent all forms of terrorist attacks. This is the case even for a small country like Israel, as demonstrated by the incessant series of suicide bombings in Israel by Palestine militants during the past few years. The problem is immensely bigger for the U.S., because of the size of its land, borders and population. It is further compounded because the U.S. is founded on freedom, and is the hub of the world economy, with tens of millions of visitors and hundreds of millions of cargo containers and packages entering the country every year. Given all this, it is actually amazing that for more than three years no dreaded attack has taken place.

Let us review major difficulties in protecting the U.S. from terrorist attacks. The discussion is to serve as a basis for subsequent discussions of the roles of technolo-
Related Content

The Impact of Network Layer on the Deadline Assignment Strategies in Distributed Real-Time Database Systems
www.irma-international.org/article/impact-network-layer-deadline-assignment/51163/

ERP System Acquisition: A Process Model and Results from an Austrian Survey
www.irma-international.org/chapter/erp-system-acquisition/18554/

Security Threats in Web-Powered Databases and Web Portals
www.irma-international.org/chapter/security-threats-web-powered-databases/28565/

Mobile Computing at the Department of Defense
www.irma-international.org/article/mobile-computing-department-defense/3263/

A Metadata Oriented Architecture for Building Datawarehouse
www.irma-international.org/article/metadata-oriented-architecture-building-datawarehouse/3269/