GUARDIAN: Geographic Utilization of Artificial Intelligence in Real-Time for Disease Identification and Notification

Michael J. Waddell, Ph.D., Shon M. Doseck, M.P.A.
Pangaea Information Technologies, Chicago Illinois
Julio C. Silva, M.D.,M.P.H., Dino P. Rumoro, D.O.
Rush University Medical Center, Chicago Illinois

BACKGROUND

Real-time disease surveillance is critical for early detection of the covert release of a biological threat agent (BTA). Numerous software applications have been developed to detect emerging disease clusters resulting from either naturally occurring phenomena or from occult acts of bioterrorism. However, these do not focus adequately on the diagnosis of BTA infection in proportion to the potential risk to public health.

GUARDIAN is a real-time, scalable, extensible, automated, knowledge-based BTA detection and diagnosis system. GUARDIAN conducts real-time analysis of multiple pre-diagnostic parameters from records already being collected within an emergency department (ED). The goal of this system is to assist clinicians in detecting potential BTAs as quickly and effectively as possible in order to better respond to and mitigate the effects of a large-scale outbreak.

GUARDIAN improves the diagnostic process by moving away from simple trend anomaly detection and towards the development of a BTA-specific infectious disease expert system [1]. Through the capture and automated application of specific clinical expertise, GUARDIAN provides the focus and accuracy necessary for effective BTA infection diagnosis. The continuity of this process improves the efficiency by which diagnoses of BTA infections can be made.

SYSTEM OVERVIEW

The GUARDIAN system currently consists of a Pre-Processor, an Inference Engine, an Alert Notification System, a Human Interaction System, a Memory Archiver and a set of relational databases managed by a Database Management System (DBMS). Figure 1 provides an overview of the current GUARDIAN system. Relational databases are illustrated using cylinders and processing components of the system are illustrated using rectangles. Interactions between components are illustrated using arrows.

The pre-processor receives HL7 messages sent to GUARDIAN, removes any individually-identifying information, and stores the HIPAA-compliant data [2] in Experiential Memory (EM). Each time new data is added to EM, the inference engine sub-system

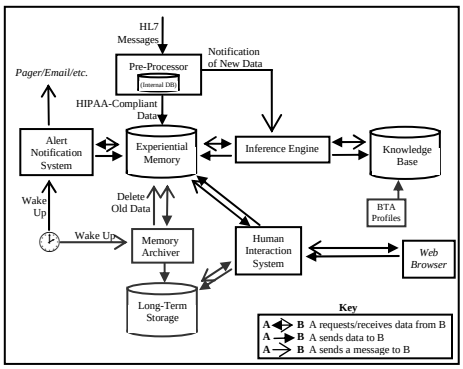

Figure 1 – System Overview

determines whether or not this new information triggers a BTA alert. If the new data represents a confirmed case of a known BTA, then the inference engine will update the parameters of the associated model accordingly. BTA alerts can be triggered either by an individual case having a probability of diagnosis that is above a BTA-specific threshold, or by a group of similar cases – clustered in time or in space – that have a probability above a separate, and generally lower, BTA-specific threshold.

The GUARDIAN system is still in active development and, as such, all of its components will be more extensively tested within the real working environment of RUMC's data center as progress continues on this work.

CONCLUSIONS

GUARDIAN effectively balances the dual challenges of early detection of individual threat agents and simultaneous detection of unusual patterns of disease occurrence in a target population. Using this system will assist clinicians in detecting potential BTAs as quickly and effectively as possible in order to better respond to and mitigate the effects of a large-scale outbreak. Active development of GUARDIAN will continue to improve and augment the capabilities of all of its subsystems. However, even in its current state, GUARDIAN is a modern, complex system that focuses adequately on the monitoring of Category A BTAs using multiple pre-diagnostic data.

REFERENCES

[1] P Jackson, Introduction to Expert Systems 3rd Edition, Addison-Wesley 1999.
[2] HIPAA Privacy Rule and Its Impacts on Research. http://privacyruleandresearch.nih.gov. 8-4-2004.